Implicitisation de surfaces algébriques

Sébastien Bis

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Implicitisation de surfaces algébriques

Sébastien Bis

N° 4684

Décembre 2002

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4684--FR

INRIA
SOPHIA ANTIPOLIS

Implicitisation de surfaces algébriques

Sébastien Bis

Thème 2 — Génie logiciel
et calcul symbolique
Projets GALAAD

Rapport de recherche n° 4684 — Décembre 2002 — 79 pages

Résumé : Le but de ce rapport est de présenter différentes méthodes permettant l'implicitisation d'une surface paramétrée, les forces et les faiblesses de chacune d'elles, et de comparer leur efficacité. Nous nous intéressons en particulier aux méthodes suivantes : formulation de Macaulay du résultant projectif, formulation de Morley, résultant résiduel, bézoutiens, méthode des surfaces mobiles, bases de Gröbner et formule d'inversion.

Mots-clés : Géométrie, algèbre, résolution, surface, paremétrisation, résultant

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : +33 4 92 38 77 77 — Télécopie : +33 4 92 38 77 65

Implicitization of algebraic surfaces

Abstract: The aim of this report is to describe different methods for computing the implicit equation of a parameterized surface, and to analyze their strength and drawbacks. We focus on the following approaches: projective resultant formulations of Macaulay, of Morley, residual resultant, moving surfaces, Gröbner basis, inversion formula.

Key-words: Geometry, algebra, resolution, surface, rational parameterization, resultant

Table des matières

1 Introduction

Il y a classiquement 2 manières de décrire une surface algébrique : la première est de donner son équation implicite, la seconde est d'en donner, si elle existe, une paramétrisation (ici les seules paramétrisations considérées seront les représentations rationnelles. Une telle paramétrisation existe **ssi** la surface est de genre 0). Les deux ont leurs avantages et leurs inconvénients : ainsi il sera facile de représenter une surface donnée sous forme paramétrée, mais plus délicat de déterminer si un point de l'espace appartient ou non à cette surface. Au contraire une simple substitution permettra de répondre à cette question si on connaît l'équation implicite de cette surface.
Toute surface donnée par une paramétrisation rationnelle admet une équation implicite, et le problème qui consiste à déterminer celle-ci est appelé problème d'implicitisation. Le problème inverse qui consiste à trouver une représentation paramétrique d'une surface donnée sous forme implicite est appelé problème de paramétrisation.
Nous nous intéresserons seulement au problème d'implicitisation.
Une autre de ses applications est le calcul d'intersections de surfaces :
supposons que l'on ait deux surface S_1 et S_2 données par deux paramétrisations $\Psi_1 : \mathbb{C}^2 \to \mathbb{C}^3$ et $\Psi_2 : \mathbb{C}^2 \to \mathbb{C}^3$, et que l'on veuille en calculer l'intersection. Alors si on peut calculer l'équation implicite F_1 de S_1, l'intersection des deux surfaces sera donnée par $F_1(C)$ où C désigne l'ensemble des points de $\mathbb{C}^2$ vérifiant $F_1(\Psi_2) = 0$ (C'est en général une courbe de $\mathbb{C}^2$).
Notre but est de présenter différentes méthodes permettant l'implicitisation, de présenter les forces et les faiblesses de chacune d'elles, et de comparer leur efficacité.

2 Résultats préliminaires

2.1 Existence de l'équation implicite

Une surface paramétrée est donnée par une application du type :

$$\varphi = \begin{pmatrix} k^2 - W & \longrightarrow & k^3 \\ (s,t) & \mapsto & (x(s,t),y(s,t),z(s,t)) \end{pmatrix}$$

$$\text{avec} \begin{cases} \text{k corps} \\ x(s,t) = \frac{p_1(s,t)}{p_4(s,t)}, y(s,t) = \frac{p_2(s,t)}{p_4(s,t)}, z(s,t) = \frac{p_3(s,t)}{p_4(s,t)} \text{ où } p_i \in k[s,t] \\ \text{ et } PGCD(p_i, i = 1...4) = 1 \\ \\ W = \{(s,t) \in k^2 / p_4(s,t) = 0\} \end{cases}$$

Les paramétrisations issues de situations concrètes (en modélisation) sont des paramétrisations réelles : $k = \mathbb{R}$. Cependant comme $\mathbb{R}$ n'est pas algébriquement clos, on étend $\varphi = \mathbb{R}^2 - W \longrightarrow \mathbb{R}^3$ en une fonction encore notée φ qui va de $\mathbb{C}^2$-W' dans $\mathbb{C}^3$, ou $W' = \{(s,t) \in \mathbb{C}^2 / p_4(s,t) = 0\}$.
L'image de φ n'est pas en général une variété algébrique de $\mathbb{C}^3$, donc on est amené à considérer sa clôture de Zariski Z :=$\overline{im\varphi}$.

Proposition 2.1 *Z est une variété algébrique* ***irréductible****.*

Preuve :

En effet Z est irréductible ssi $\mathcal{I}$(Z) :={P$\in \mathbb{C}[x,y,z] / P(Z) = 0$} est un idéal premier, ce que nous allons montrer. Soit P$\in \mathcal{I}(Z)$. On a donc P(im φ)=0, ie $P(\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_3(s,t)}{p_4(s,t)}) =$ 0 pour tout (s,t)$\in (C)^2 - W'$.
On peut choisir un entier α suffisamment grand pour que $(p_4(s,t))^\alpha \cdot P(\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_3(s,t)}{p_4(s,t)})$ soit en fait un polynôme de $\mathbb{C}[s,t]$. Ce dernier polynôme définit alors une fonction polynomiale nulle sur tout $\mathbb{C}^2$, donc est le polynôme nul.
On a donc montré :

$$P \in \mathcal{I}(Z) \Leftrightarrow \exists \alpha \in \mathbb{N} / (p_4)^\alpha \cdot P \circ \varphi = 0 \in \mathbb{C}[s,t]$$

(l'implication inverse étant évidente).
Soit A,B $\in \mathbb{C}[s,t]$ tels que $A \cdot B \in \mathcal{I}(Z)$.
Pour montrer que $\mathcal{I}(Z)$ est premier il faut prouver que $A \in \mathcal{I}(Z)$ ou $B \in \mathcal{I}(Z)$. Or on vient de voir que

$$\begin{aligned} A \cdot B \in \mathcal{I}(Z) &\Leftrightarrow \exists \alpha \in \mathbb{N} / (p_4)^\alpha \cdot (AB) \circ \varphi = 0 \in \mathbb{C}[s,t] \\ &\Leftrightarrow \exists \alpha \in \mathbb{N} / [(p_4)^\alpha \cdot A \circ \varphi] \cdot [(p_4)^\alpha \cdot B \circ \varphi] = 0 \in \mathbb{C}[s,t] \end{aligned}$$

Or $\mathbb{C}[s,t]$ est intègre, donc $(p_4)^\alpha \cdot A \circ \varphi$ ou $(p_4)^\alpha \cdot B \circ \varphi$ est le polynôme nul, i.e. $A \in \mathcal{I}(Z)$ ou $B \in \mathcal{I}(Z)$. CQFD.

Z est donc une variété algébrique de $\mathbb{C}^3$, qui est de plus de dimension 2 car on a

supposé que la paramétrisation donnait une surface. Alors il existe $F \in \mathbb{C}[x,y,z]$ irréductible tel que $Z = V(F)$. Ceci provient du résultat suivant :

Proposition 2.2 *Soit Z une variété algébrique de $\mathbb{C}^n$ de dimension n-1.*
Alors il existe f polynôme irréductible de $\mathbb{C}[t_1,...,t_n]$ tel que Z=V(f).

Preuve :

Z est a priori de la forme $V(f_1,...,f_r)$ avec $f_i \in \mathbb{C}[t_1,...,t_n]$ et $f_i \neq 0$. Choisissons les f_i tel que r soit minimal. On peut toujours se ramener au cas où les f_i sont irréductibles : supposons par exemple que f_1 soit réductible et s'écrive $f_1 = gh$ avec $g,h \in \mathbb{C}[t_1,...,t_n]$. Alors $Z = V(g,f_2,...,f_r) \cup V(h,f_2,...,f_r)$, et comme Z est irréductible on a $Z = V(g,f_2,...,f_r)$ ou $Z = V(g,f_2,...,f_r)$.
En itérant le processus on se ramène donc au cas ou les f_i sont irréductibles.
Montrons maintenant que r=1 :
supposons $r \geq 2$. Comme $V(f_1)$ est de dimension n-1 (car $f_1 \neq 0$), et que$Z = V(f_1,...,f_r)$ est aussi de dimension n-1 (par hypothèse), on en déduit que l'on doit avoir $dim(V(f_1,f_r)) = n-1$. Ceci implique que f_r est un diviseur de zéro dans $\frac{\mathbb{C}[t_1,...,t_n]}{(f_1)}$ (cf [Cox1], chap 9). Mais comme f_1 est irréductible, $\frac{\mathbb{C}[t_1,...,t_n]}{(f_1)}$ est intègre et donc f_r est un multiple de f_1. Par conséquent $V(f_1,...,f_r) = V(f_1,...,f_{r-1})$ et r n'est pas minimal.
Donc r=1. CQFD.

Z s'écrit donc $Z = V(F)$, et F est *l'équation implicite (irréductible) de la surface* (jusque là on avait pas encore démontré son existence).

2.2 Paramétrisation propre/impropre, point base et degré de l'équation implicite

Il n'existe jamais de paramétrisation rationnelle unique pour une surface donnée. Par exemple considérons la paramétrisation affine de la sphère unité de $\mathbb{C})^3$:

$$\varphi : (s,t) \mapsto (\frac{1-s^2-t^2}{1+s^2+t^2}, \frac{2s}{1+s^2+t^2}, \frac{2t}{1+s^2+t^2}).$$

En faisant $s = uv$ et $t = u^2$ on obtient une nouvelle paramétrisation de la sphère unité :

$$\psi : (u,v) \mapsto (\frac{1-u^2v^2-u^4}{1+u^2v^2+u^4} \frac{1-u^2v^2-u^4}{1+u^2v^2+u^4}, \frac{2uv}{1+u^2v^2+u^4}, \frac{2u^2}{1+u^2v^2+u^4}).$$

La première paramétrisation est toutefois bien meilleure, car elle est **propre**, i.e. elle induit une bijection entre un ouvert dense de l'espace des paramètres et un ouvert dense de la surface.
La seconde, qui n'est pas propre, est dite **impropre** : sur cet exemple un point générique de la sphère unité de $\mathbb{C}^3$ à deux antécédents par ψ.
Par ailleurs une paramétrisation impropre fait toujours intervenir des polynômes de plus haut degré (comme sur l'exemple), et donc engendre des calculs plus compliqués.
Toute surface rationnelle possède une paramétrisation propre [Castelnuovo], bien qu'actuellement aucun algorithme ne permette de la déterminer à partir d'une paramétrisation impropre. Des méthodes sont toutefois connues pour déterminer si une paramétrisation est propre ou non [PDSS, Baj, Hoff].

Nous avons évoqué au paragraphe précédent la nécessité de considérer les paramétrisations non pas sur $\mathbb{R}$, mais sur $\mathbb{C}$. Ceci ne suffit pas toujours, et l'on peut avoir besoin de considérer des points à l'infini, par exemple pour pouvoir appliquer le théorème de Bezout (cf. plus loin). On peut donc étendre une paramétrisation

$$\varphi = \begin{pmatrix} \mathbb{C}^2 - W & \longrightarrow & \mathbb{C}^3 \\ (s,t) & \mapsto & (\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_1(s,t)}{p_4(s,t)}) \end{pmatrix} \text{ en}$$

$$\varphi = \begin{pmatrix} \mathbb{P}^2 - W_1 & \longrightarrow & \mathbb{P}^3 \\ (s,t,u) & \mapsto & (\overline{p_1}(s,t,u) : \overline{p_2}(s,t,u) : \overline{p_3}(s:t:u) : \overline{p_4}(s,t,u)) \end{pmatrix}$$

où

$$\begin{cases} W = \{(s,t) \in k^2 / p_4(s,t) = 0\}, \\ \text{les } \overline{p_i} \text{ désignent les polynômes de degré d obtenus par homogénéisation} \\ \text{des } p_i, \text{où d désigne le plus grand des degrés des } p_i, \\ W_1 = \{(s,t,u) \in \mathbb{P}^2 / \overline{p_i}(s,t,u) = 0, i = 1...4\} = V(\overline{p_1}, \overline{p_2}, \overline{p_3}, \overline{p_4}). \end{cases}$$

Définition 2.1 *Un* point base *est une solution commune aux polynômes homogènes* $\overline{p_1}, \overline{p_2}, \overline{p_3}, \overline{p_4}$.

L'ensemble des points bases est donc ce que l'on a appelé W_1, et qui correspond aux points de $\mathbb{P}^2$ où la paramétrisation n'est pas définie. Comme $PGCD(\overline{p_1}, \overline{p_2}, \overline{p_3}, \overline{p_4}) = 1$ (car $PGCD(p_1, p_2, p_3, p_4) = 1$), il n'y a qu'un nombre fini de points bases.
Chaque p_i détermine une courbe de $\mathbb{P}^2$ en faisant $p_i = 0$. La multiplicité d'un point base est définie comme étant égale au minimum des multiplicités de chacune de ces quatre courbes $p_i = 0$ en ce point. A chaque point base on peut associer une courbe rationnelle de la surface, courbe qui est en quelque sorte un "éclatement" du point

base.
Ce phénomène s'explique ainsi :
Considérons la paramétrisation rationnelle :
$\varphi(s,t,u) = (su + 2tu + s^2, su + 3tu + t^2, su + tu + 2st + 4tu)$.
$P = (0,0,1)$ en est un point base.
Regardons ce qui se passe lorsque l'on s'approche de P selon une direction fixée, c'est-à-dire en parcourant une droite donnée passant par P. Plaçons nous dans la carte u=1. Fixons m, et approchons nous de P tout en restant sur la droite s=mt. On a :

$$\begin{aligned} \mathrm{G(m)} &:= lim_{t\to 0}\varphi(mt,t,1) \\ &= lim_{t\to 0}(mt + 2t + m^2t^2, mt + 3t + t^2, mt + t + 2mt^2, mt + 4t) \\ &= lim_{t\to 0}(m + 2 + m^2t, m + 3 + t, m + 1 + 2mt, m + 4) \\ &= (\mathrm{m{+}2,\ m{+}3,\ m{+}1,\ m{+}4}) \end{aligned}$$

$m \to G(m)$ est la paramétrisation rationnelle d'une droite de la surface. Ainsi à chaque direction autour du point base correspond un point de l'adhérence de l'image de la paramétrisation.
Ce que l'on a fait sur cet exemple se généralise sans problème et montre donc qu'un point base "éclate" en une courbe rationnelle de la surface, courbe appelée "seam curve" en anglais. L'ensemble des points de ces "seam curves" correspond à l'ensemble des points de la surface qui ne sont pas atteints par la paramétrisation. Les points bases jouent un rôle capital en modélisation car leur existence complique fortement le problème de l'implicitisation, comme nous le verrons plus loin.

Remarque : Soit $\varphi = \mathbb{P}^2 \longrightarrow \mathbb{P}^3$ une paramétrisation propre et sans point base d'une surface S, et soit $\psi = \mathbb{P}^2 \longrightarrow \mathbb{P}^3$ une paramétrisation impropre de S du type $\psi = \varphi \circ \alpha$ avec $\alpha = \mathbb{P}^2 \longrightarrow \mathbb{P}^2$. Alors il est possible que ψ ait des points bases, comme le montre l'exemple suivant :
$\varphi(p,q,r) = (x,y,z,w) = (p + r, 2p + q, q - 3r, q + r)$.
$\alpha(p,q,r) = (st + t^2, su + tu, s^2 + su)$.
$\psi(s,t,u) = \varphi \circ \alpha = (x,y,z,w)$
$= (s^2 + t^2 + st + su, 2t^2 + 2st + su + tu, -3s^2 - 2su + tu, s^2 + tu + 2su)$.
φ n'a pas de point base mais (0,0,1) est un point base de ψ.

Nous pouvons maintenant aborder la question du degré de l'équation implicite d'une surface paramétrée par une application $\varphi = \mathbb{P}^2 \longrightarrow \mathbb{P}^3$. On va voir que ce degré dépend du nombre de points bases de φ.

Supposons que la paramétrisation soit propre :
le degré de l'équation implicite d'une surface peut être vu comme le nombre de points d'intersection entre la surface et une droite générique notée D ([Shaf]). Une droite générique de $\mathbb{P}^3$ s'écrit comme une intersection de 2 plans :

$$a_1x + a_2y + a_3z + a_4w = 0 \quad (1)$$
$$b_1x + b_2y + b_3z + b_4w = 0 \quad (2)$$

Si φ s'écrit $\varphi(s,t,u) = (p_1(s,t,u),p_2(s,t,u),p_3(s,t,u),p_4(s,t,u))$ avec les p_i des polynômes homogènes de degré n, les points d'intersection entre la surface et la droite D sont alors donnés par les points d'intersection entre les deux courbes de $\mathbb{P}^2$ suivantes :

$$a_1p_1(s,t,u) + a_2p_2(s,t,u) + a_3p_3(s,t,u) + a_4p_4(s,t,u) = 0 \quad (3)$$
$$b_1p_1(s,t,u) + b_2p_2(s,t,u) + b_3p_3(s,t,u) + b_4p_4(s,t,u) = 0 \quad (4)$$

Ces courbes sont de degré n en s,t,u, donc d'après le théorème de Bezout elles s'intersectent en n^2 points (comptés avec multiplicité). Si la paramétrisation n'a pas de point base, chacun de ses n^2 points correspond alors à un antécédent d'un point de la surface qui intersecte la droite D, et l'équation implicite est donc de degré n^2.
Si par contre la paramétrisation contient un point base, alors celui-ci fait forcément partie des n^2 points d'intersection de (3) et (4), mais il ne correspond pas à un antécédent d'un point de la surface : D intersecte donc S en $n^2 - 1$ points, ou moins (on suppose pour cela que D ne coupe pas la surface en un point qui serait sur une des "seam curves" de S, et donc chacun des points de $S \cap D$ correspond bien à un point de la paramétrisation. Ceci est possible car il n'y a qu'un nombre fini de "seam curves"et qu'elles sont de dimension 1 : une droite générique ne passe donc pas par elles). Si il y a p points bases simples, alors le degré de l'équation implicite est $n^2 - p$. Les points bases de multiplicités k font quand à eux baisser le degré de l'équation implicite au moins de k^2, et au moins de $k^2 + 1$ si (3) et (4) s'intersectent tangentiellement au point en question [Sed90].
Terminons ce paragraphe en évoquant le cas des surfaces paramétrées par des polynômes de type $p_k(s,t) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j}^k s^i t^j$
(où $p_i(s,t,u) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} s^i t^j u^{n+m-i-j}$ en notation homogène) pour $k = 1,2,3,4$.
Les p_k sont dit "polynômes de bidegré (m,n)", càd qu'ils sont de degré total $m + n$ mais de degré seulement m en s et de degré seulement n en t.
Ce type de polynômes intervient très fréquemment en CAO (conception assistée par ordinateur).
Une telle paramétrisation admet toujours comme point base $(1 : 0 : 0)$ avec multiplicité n et $(0 : 1 : 0)$ avec multiplicité m.

D'après ce que l'on a dit précédemment, le degré de l'équation implicite de la surface est au plus $(n+m)^2 - n^2 - m^2 = 2mn$, et de degré $< 2mn$ si la paramétrisation admet d'autres points bases ou si les courbes données par (3),(4) s'intersectent tangentiellement en $(1:0:0)$ ou en $(0:1:0)$.

3 Premières méthodes d'implicitisation

De nombreuses méthodes méthodes d'implicitisation font appel soit à la théorie des résultants, soit à la théorie des bases de Gröbner. Nous allons donc dans ce chapitre présenter le principe de ces méthodes.

3.1 Implicitisation et résultants

Le premier outil fondamental pour le problème de l'implicitisation est la théorie des résultants. Nous allons commencer par faire quelques rappels : (pour les détails voir [BEM])

$$(S) = \begin{cases} f_0(\mathbf{x}) = \sum_{j=1}^{k_0} c_{0,j}\psi_{0,j}(\mathbf{x}) \\ \vdots \\ f_n(\mathbf{x}) = \sum_{j=1}^{k_n} c_{n,j}\psi_{n,j}(\mathbf{x}) \end{cases}$$

Soit (S) un système de $(n+1)$ équations dans $\mathbb{P}^n$, où les $\mathbf{c} = (c_{i,j})$ sont des paramètres, $\mathbf{x} = (x_0 : \ldots : x_n)$ est un point de $\mathbb{P}^n$, et où les $\psi_{n,j}(\mathbf{x})$ sont des polynômes homogènes indépendants des paramètres $\mathbf{c}$ avec degré $\text{total}(\psi_{i,j}) = d_i \in \mathbb{N}$.
On cherche à quelles conditions sur $\mathbf{c}$ ce système admet au moins une solution dans $\mathbb{P}^n$.

Théorème 3.1 *Si pour tout point* $\mathbf{x} \in \mathbb{P}^n$, *et pour tout* $i = 0,\ldots,n$ *le vecteur* $(\psi_{i,0}(\mathbf{x}),\ldots,\psi_{i,k_i}(\mathbf{x}))$ *n'est pas nul ALORS il existe un unique polynôme* $Res_{(f_1,\ldots,f_n)} \in \mathbb{Z}[c_{i,j}]$ *tel que*
1) le système (S) *admet une solution dans* $\mathbb{P}^n$ *pour une spécialisation des coefficients* $(c_{i,j})$ ***ssi*** $Res_{(f_1,\ldots,f_n)} = 0$ *pour cette spécialisation*
2)$Res_{(x_0^{d_0},\ldots,x_n^{d_n})} = 1$
3)$Res_{(f_1,\ldots,f_n)}$ *est irréductible dans* $\mathbb{Z}[c_{i,j}]$, *et même dans* $\mathbb{C}[c_{i,j}]$
Ce polynôme est appelé le résultant *de* $f_1,\ldots,f_n$.

En particulier le résultant de

$$(S) = \begin{cases} f_0(\mathbf{x}) = \sum_{\alpha_0+\ldots+\alpha_n=d_0} c_{0,\alpha} x_0^{\alpha_0} \ldots x_n^{\alpha_n} \\ \vdots \\ f_n(\mathbf{x}) = \sum_{\alpha_0+\ldots+\alpha_n=d_n} c_{n,\alpha} x_0^{\alpha_0} \ldots x_n^{\alpha_n} \end{cases}$$

est bien défini.
Rappelons comment on le construit (construction de Macaulay) : Posons $d = \sum_{i=0}^{n}(d_i - 1) + 1$. Soit S l'ensemble des monômes de $\mathbb{C}[x_0, \ldots, x_n]$ de degré d. S est l'union disjointes des ensembles suivants :
$S_0 = \{x^\alpha / |\alpha| = d,\ x_0^{d_0} \text{ divise } x^\alpha\}$
$S_1 = \{x^\alpha / |\alpha| = d,\ x_0^{d_0} \text{ ne divise pas } x^\alpha \text{ mais } x_1^{d_1} \text{ divise } x^\alpha\}$
$\vdots$
$S_n = \{x^\alpha / |\alpha| = d,\ x_0^{d_0}, \ldots, x_{n-1}^{d_{n-1}} \text{ ne divise pas } x^\alpha \text{ mais } x_n^{d_n} \text{ divisent } x^\alpha\}$

On construit ensuite $\binom{n+d}{n}$ équations polynomiales de degré total $\binom{n+d}{n}$:

$$(E) = \begin{cases} x^\alpha / x_0^{d_0} f_0 = 0 \text{ pour tout } \alpha \in S_0 \\ \vdots \\ x^\alpha / x_n^{d_n} f_0 = 0 \text{ pour tout } \alpha \in S_n \end{cases}$$

Ce système peut être vu comme un système à $\binom{n+d}{n}$ équations (à coefficients dans $\mathbb{Z}[c_{i,j}]$) et à $\binom{n+d}{n}$ inconnues, où les inconnues sont les monômes de degré total d.
La matrice des coefficients de ce système est appelée matrice de Macaulay de $f_0, \ldots, f_n$. Son déterminant est noté D_n : c'est un polynôme de $\mathbb{Z}[c_{i,j}]$. On vérifie que pour $f_0 = x_0^{d_0}, \ldots, f_n = x_n^{d_n}$, D_n vaut ± 1 (en particulier D_n n'est pas nul). Par construction, si pour une spécialisation des $c_{i,j}$ le résultant s'annule, alors $f_i = 0$, $i = 0, \ldots, n$ admet une solution, et donc (E) aussi, ce qui implique que D_n s'annule pour cette spécialisation; donc comme Res est un polynôme irréductible de $\mathbb{C}[c_{i,j}]$ (et que $\mathbb{C}$ est algébriquement clos), D_n est un multiple de Res.
On remarque que D_n est homogène de degré $d_1 \ldots d_n$ en les coefficients de f_n. Par ailleurs on peut montrer que $Res_{(f_1,\ldots,f_n)}$ est un polynôme homogène en les coefficients de f_i de degré $d_1 \ldots d_n$, donc on a

$$D_n = Res_{(f_1,\ldots,f_n)} \cdot G$$

où G est un polynôme en les coefficients des $f_1, \ldots, f_n$.
On déduit de tout cela que, si on note D_i de déterminant de la matrice de Macaulay de $f_{i+1}, \ldots, f_n, f_1, \ldots, f_i$ on a

$$Res_{(f_1,\ldots,f_n)} = \pm PGCD(D_0, \ldots, D_n)$$

On peut aussi montrer que G est le déterminant d'une sous matrice carrée de la matrice de Macaulay de $(f_1, \ldots, f_n)$: ([Mac02])

Soit D'_n la sous-matrice de la matrice de Macaulay de $(f_0,\ldots,f_n)$ obtenue en supprimant toutes les lignes et les colonnes correspondant à des monômes x^α qui ne sont divisibles que par un seul des x^{d_i}. Alors :

$$Res_{(f_1,\ldots,f_n)} = \pm D_n/D'_n$$

Cette seconde expression du résultant est moins coûteuse à calculer que la précédente.

Remarque : comme le nombre de monômes qui ne sont divisibles que par un seul des d_i est $\sum_0^n \frac{d_0\ldots d_n}{d_i}$, $Res_{(f_1,\ldots,f_n)}$ est de degré total $\sum_0^n \frac{d_0\ldots d_n}{d_i}$.

Faisons maintenant le lien entre la théorie des résultants et notre sujet :
soit S une surface paramétrée par

$$\varphi = \left(\begin{array}{ccc} \mathbb{P}^2 & \longrightarrow & \mathbb{C}^3 \\ (s:t:u) & \mapsto & (\frac{p_1(s:t:u)}{p_4(s:t:u)},\frac{p_2(s:t:u)}{p_4(s:t:u)},\frac{p_1(s:t:u)}{p_4(s:t:u)}) \end{array} \right)$$

où p_1,p_2,p_3,p_4 sont quatre polynômes de degré total d. Posons comme précédemment :

$$H_1(s,t,u) = p_4(s,t,u)x - p_1(s,t,u) \tag{5}$$
$$H_2(s,t,u) = p_4(s,t,u)y - p_2(s,t,u) \tag{6}$$
$$H_3(s,t,u) = p_4(s,t,u)z - p_3(s,t,u) \tag{7}$$

Les coefficients des H_i sont des polynômes de degré 1 en les variables x,y,z.Donc $Res_{(H_1,H_2,H_3)}$ est un polynôme de $\mathbb{C}[x,y,z]$ qui s'annule pour une spécialisation x_0,y_0,z_0 des x,y,z **ssi** il existe $(s_0,t_0,u_0) \in \mathbb{P}^2$ tel que

$$(S) = \left\{ \begin{array}{l} p_4(s_0,t_0,u_0)x - p_1(s_0,t_0,u_0) = 0 \\ p_4(s_0,t_0,u_0)y - p_2(s_0,t_0,u_0) = 0 \\ p_4(s_0,t_0,u_0)z - p_3(s_0,t_0,u_0) = 0 \end{array} \right.$$

Supposons qu'il n'y ait pas de point base. Cela implique que $p_4(s_0,t_0,u_0) \neq 0$ et donc

$$x_0 = \frac{p_1(s_0,t_0)}{p_4(s_0,t_0)} \quad y_0 = \frac{p_2(s_0,t_0)}{p_4(s_0,t_0)} \quad z_0 = \frac{p_3(s_0,t_0)}{p_4(s_0,t_0)}$$

Autrement dit si il n'y a pas de point base, $Res_{(H_1,H_2,H_3)}$ est un polynôme de $\mathbb{C}[x,y,z]$ qui s'annule en $(x_0,y_0,z_0) \in \mathbb{C}^3$ **ssi** $(x_0,y_0,z_0) \in Im\varphi$. Donc $Res_{(H_1,H_2,H_3)}$ est de la forme

$$Res_{(H_1,H_2,H_3)}(x,y,z) = (F(x,y,z))^k$$

où F désigne l'équation implicite de S, $k \in \mathbb{N} - \{0\}$.

Remarque 1 : k correspond au nombre d'antécédents que possède un point générique de $Im\varphi$. Si la paramétrisation est propre $k = 1$.

Remarque 2 : $Res_{(H_1,H_2,H_3)}(x,y,z)$ fournit donc une équation implicite non réduite a priori (si il n'y a pas de point base). Si l'on veut F exactement il suffit d'utiliser le fait que si $Res_{(H_1,H_2,H_3)}$ est de degré > 0 en r avec r=x,y ou z, alors $F = PGCD\big(Res_{(H_1,H_2,H_3)}, \frac{\partial}{\partial r} Res_{(H_1,H_2,H_3)}\big)$. C'est ce que fait la procédure *squarefree* de MAPLE.

Que se passe-t-il quand il y a des points bases?
Un point base sera toujours solution de H_1,H_2,H_3, et ce pour toutes valeurs de x,y,z. Le résultant sera donc identiquement nul. Cette méthode est donc efficace seulement si il n'y a pas de point base. Toutefois si elle est théoriquement satisfaisante dans ce cas, elle ne l'est pas pratiquement : en effet, idéalement pour appliquer cette méthode il faudrait calculer le résultant symbolique de trois polynômes homogènes génériques de degré d, puis remplacer les coefficients génériques des f_i par les coefficients particuliers des H_i. Or le calcul du résultant symbolique est très long car il nécessite de calculer des déterminants génériques de taille $\binom{d+2}{d} = \frac{(d+2)(d+1)}{2}$, ce qui est extrêmement coûteux.
On préfère donc calculer D_n/D'_n directement avec les coefficients des H_i, mais ce calcul reste quand même assez coûteux, et de plus il est alors possible que D_n et D'_n s'annulent simultanément (cf les exemples de la section 10), ce qui rend impossible le calcul de D_n/D'_n (du moins sans avoir recours à des techniques de perturbations).

Évoquons pour terminer le cas du résultant de 3 polynômes de bidegré (m,n) :

$$\begin{cases} f(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} s^i t^j \\ g(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} s^i t^j \\ h(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} c_{i,j} s^i t^j \end{cases}$$

On a déjà vu que trois polynômes de ce type avaient toujours des zéros communs à l'infini :
$(1 : 0 : 0)$ avec multiplicité n
$(0 : 1 : 0)$ avec multiplicité m.
Leur résultant classique s'annule donc toujours.
On cherche s'il existe un résultant "conditionnel" qui serait un polynôme en les coef-

ficients de f,g,h et qui s'annulerait **ssi** f,g et h ont une solution commune autre que leurs solutions canoniques. Par le théorème de Bezout deux des trois polynômes f,g et h ont génériquement $(m+n)^2$ points d'intersections, donc jusqu'à $(n+m)^2 - n^2 - m^2 = 2mn$ solutions communes non canoniques. Chacune de ces solutions induisant une relation linéaire sur les coefficients du troisième polynôme, on en déduit que si un résultant "conditionnel" de f,g et h existe, il doit être de degré $2mn$ en les coefficients de chacun des trois polynômes.
Un tel résultant "conditionnel" existe, et il est donné par le déterminant de la matrice de Dixon de f,g,h : considérons le déterminant :

$$\Delta(s,t,\alpha,\beta) = \begin{vmatrix} f(s,t) & g(s,t) & h(s,t) \\ f(\alpha,t) & g(\alpha,t) & h(\alpha,t) \\ f(\alpha,\beta) & g(\alpha,\beta) & h(\alpha,\beta) \end{vmatrix}$$

et le quotient

$$\delta(s,t,\alpha,\beta) = \frac{\Delta(s,t,\alpha,\beta)}{(s-\alpha)(t-\beta)}$$

Comme $\Delta(s,t,\alpha,\beta) = 0$ quand $s = \alpha$ ou $t := \beta$, $(s-\alpha)(t-\beta)$ divise le numérateur $\Delta(s,t,\alpha,\beta)$. $\delta(s,t,\alpha,\beta)$ est donc un polynôme de degré $(m-1)$ es s et $(2m-1)$ en t. On peut écrire ce polynôme sous forme matricielle :

$$\begin{pmatrix} \alpha^{2m-1}\beta^{n-1} \\ \vdots \\ \alpha^{2m-1} \\ \vdots \\ \beta^{n-1} \\ \vdots \\ 1 \end{pmatrix}^T Dix(f,g,h) \begin{pmatrix} s^{m-1}t^{2n-1} \\ \vdots \\ s^{m-1} \\ \vdots \\ t^{2n-1} \\ \vdots \\ 1 \end{pmatrix}$$

où $Dix(f,g,h)$ est une matrice de taille $2mn$ (appelée matrice de Dixon de f,g,h). Comme

$$\Delta(s,t,\alpha,\beta) = \sum_{i,k,p=0}^{m} \sum_{j,l,q=0}^{n} |i;j;k;l;p;q| s^i t^{j+l} \alpha^{k+p} \beta^q$$

avec

$$|i;j;k;l;p;q| = \begin{vmatrix} a_{i,j} & b_{i,j} & c_{i,j} \\ a_{k,l} & b_{k,l} & c_{k,l} \\ a_{p,q} & b_{p,q} & c_{p,q} \end{vmatrix}$$

les coefficients de $Dix(f,g,h)$ sont des sommes de déterminants $|i;j;k;l;p;q|$, et $det(Dix(f,g,h)) = |Dix(f,g,h)|$ est un polynôme de degré total $6mn$ et de degré $2mn$ en les coefficients de f,g ou h.

Proposition 3.1 *$|Dix(f,g,h)|$ s'annule pour une spécialisation des $a_{i,j}$,$b_{i,j}$,$c_{i,j}$* ***ssi*** *pour cette spécialisation f,g et h ont une solution commune autre que leurs solutions communes canoniques.*

Les étapes de la démonstration de cette proposition sont les mêmes que celles de la démonstration pour la formulation du résultant de Macaulay :

1) $|Dix(f,g,h)|$ s'annule si f,g et h ont une solution commune :
si (s_0,t_0) est une solution de f,g et h, alors $\Delta(s_0,t_0,\alpha,\beta) = 0$ et donc $\delta(s_0,t_0,\alpha,\beta)$ est nul (vu comme un polynôme en α et β). Ceci se traduit matriciellement par

$$Dix(f,g,h) \begin{pmatrix} s_0^{m-1}t_0^{2n-1} \\ \vdots \\ s_0^{m-1} \\ \vdots \\ t_0^{2n-1} \\ \vdots \\ 1 \end{pmatrix} = 0$$

donc 0 est valeur propre de $Dix(f,g,h)$ et donc $|Dix(f,g,h)| = 0$

2) $|Dix(f,g,h)|$ n'est pas le polynôme nul (on le prouve en spécialisant les coefficients).

3) $|Dix(f,g,h)|$ a "le bon degré" en les coefficients de f,g et h, càd $2mn$ en les coefficients de f, de g, et de h.

Grâce au résultant de Dixon on va pouvoir implicitiser une surface donnée par 4 polynômes de bidegré (m,n) n'ayant pas de point base (lorsque l'on dit "sans point base" en parlant d'une paramétrisation par des polynômes de bidegré (m,n) on sous-entend évidemment "sans point base autre que les points bases canoniques à l'infini inhérents à ce type de paramétrisation).

Soit S une surface paramétrée par

$$\varphi = \left(\begin{array}{ccc} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^3 \\ (s,t) & \mapsto & (\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_1(s,t)}{p_4(s,t)}) \end{array} \right)$$

avec

$$\left\{ \begin{array}{l} p_1(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} s^i t^j \\ p_2(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} s^i t^j \\ p_3(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} c_{i,j} s^i t^j \\ p_4(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} d_{i,j} s^i t^j \end{array} \right.$$

On pose

$$\left\{ \begin{array}{l} H_1(s,t,x,y,z) = p_4(s,t)x - p_1(s,t) \\ H_2(s,t,x,y,z) = p_4(s,t)y - p_2(s,t) \\ H_3(s,t,x,y,z) = p_4(s,t)z - p_3(s,t) \end{array} \right.$$

Si il n'y a pas de point base, le résultant de Dixon de H_1,H_2,H_3 est un polynôme en x,y,z qui s'annule en (x_0,y_0,z_0) **ssi** (x_0,y_0,z_0) est un point de S. Donc $|Dix(H_1,H_2,H_3)| = 0$ **est une puissance de l'équation implicite de S**.

Remarque : on a vu que le degré de l'équation implicite de S est $2mn$ (cf paragraphe 2.2). Montrons que l'on retrouve bien ce résultat à l'aide du résultant de Dixon :
un coefficient de la matrice $Dix(H_1,H_2,H_3)$ est une somme de déterminant de type :

$$\left| \begin{array}{ccc} a_{i,j} - xd_{i,j} & b_{i,j} - yd_{i,j} & c_{i,j} - zd_{i,j} \\ a_{k,l} - xd_{k,l} & b_{k,l} - yd_{k,l} & c_{k,l} - zd_{k,l} \\ a_{p,q} - xd_{p,q} & b_{p,q} - yd_{p,q} & c_{p,q} - zd_{p,q} \end{array} \right|$$

Par multilinéarité ce résultant est égal à :

$$xyz \left| \begin{array}{ccc} -d_{i,j} & -d_{i,j} & -d_{i,j} \\ -d_{k,l} & -d_{k,l} & -d_{k,l} \\ -d_{p,q} & -d_{p,q} & -d_{p,q} \end{array} \right| + xy \left| \begin{array}{ccc} -d_{i,j} & -d_{i,j} & c_{i,j} \\ -d_{k,l} & -d_{k,l} & c_{k,l} \\ -d_{p,q} & -d_{p,q} & c_{p,q} \end{array} \right| + \ldots$$

$$\ldots + z \left| \begin{array}{ccc} a_{i,j} & b_{i,j} & -d_{i,j} \\ a_{k,l} & b_{k,l} & -d_{k,l} \\ a_{p,q} & b_{p,q} & -d_{p,q} \end{array} \right| + \left| \begin{array}{ccc} a_{i,j} & b_{i,j} & c_{i,j} \\ a_{k,l} & b_{k,l} & c_{k,l} \\ a_{p,q} & b_{p,q} & c_{p,q} \end{array} \right|$$

Dans ce polynôme en x,y,z tous les coefficients des termes de degré total en x,y,z strictement supérieur à 1 sont nuls.
Ainsi les coefficients de $Dix(H_1,H_2,H_3)$ sont linéaires en x,y,z.
Comme $Dix(H_1,H_21,H_3)$ est de taille $2mn$, $|Dix(H_1,H_21,H_3)|$ est bien de degré total $2mn$.

3.2 Implicitisation et bases de Gröbner

Le deuxième outil classique dont on dispose pour le problème de l'implicitisation est les bases de Gröbner. Nous allons commencer là aussi par faire quelques rappels [Cox1, chap.3] :

Théorème 3.2 *Soit* $f_1,\ldots,f_s \in \mathbb{C}[X_1,\ldots,X_n]$ *et* $Z = V(f_1,\ldots,f_s) \subset \mathbb{C}^n$.
Soient I_l *le l-ième idéal d'élimination de* I $(1 \leq l \leq n)$,

$$i.e. \quad I_l = I \cap \mathbb{C}[X_{l+1},\ldots,X_n].$$

Soit π_l *la projection :* $\varphi = \begin{pmatrix} \mathbb{C}^n & \longrightarrow & \mathbb{C}^{n-l} \\ (x_1,\ldots,x_n) & \mapsto & (x_{l+1},\ldots,x_n) \end{pmatrix}$.
ALORS le plus petit ensemble algébrique contenant $\pi_l(Z)$, *ie la clôture de Zariski de* $\pi_l(Z)$ *est* $V(I_l)$:

$$\overline{\pi_l(Z)} = V(I_l)$$

On rappelle au passage comment calculer I_l :
Soit $\{g_1,\ldots,g_r\}$ une base de Gröbner pour l'ordre lexicographique où $X_1 > \ldots > X_n$. Alors une base de Gröbner de I_l est

$$\{g_1,\ldots,g_r\} \cap \mathbb{C}[X_{l+1},\ldots,X_n].$$

Revenons à notre problème d'implicitisation :
Soit S une surface paramétrée par

$$\varphi = \begin{pmatrix} \mathbb{C}^2 - W & \longrightarrow & \mathbb{C}^3 \\ (s,t) & \mapsto & (\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_1(s,t)}{p_4(s,t)}) \end{pmatrix} \text{ où } W = V(p_4).$$

Supposons qu'il n'y ait pas de point base dans le domaine affine. Considérons les trois polynômes de $\mathbb{C}[s,t,x,y,z]$:

$$H_1(s,t,x,y,z) = p_4(s,t)x - p_1(s,t) \tag{8}$$
$$H_2(s,t,x,y,z) = p_4(s,t)y - p_2(s,t) \tag{9}$$
$$H_3(s,t,x,y,z) = p_4(s,t)z - p_3(s,t) \tag{10}$$

Soit $Z := V(I) \subset \mathbb{C}^5$ où $I = \langle H_1,H_2,H_3\rangle \subset \mathbb{C}[s,t,x,y,z]$.
Avec les notations du théorème on a : $\pi_{\mathbf{2}}(\mathbf{Z}) = \mathbf{Im}(\varphi)$.
En effet : soit $(s_0,t_0,x_0,y_0,z_0) \in Z$. Comme il n'y a pas de point base dans le domaine affine on a forcément $p_4(s_0,t_0) \neq 0$, et donc

$$x_0 = \frac{p_1(s_0,t_0)}{p_4(s_0,t_0)}, \quad y_0 = \frac{p_2(s_0,t_0)}{p_4(s_0,t_0)} \quad ,z_0 = \frac{p_3(s_0,t_0)}{p_4(s_0,t_0)}$$

Donc $\pi_2((s_0,t_0,x_0,y_0,z_0)) \in Im\varphi$.
L'autre inclusion est évidente.

D'après le théorème rappelé ci-dessus,on a donc $\overline{Im\varphi} = V(I_2)$. Or $\overline{Im\varphi} = V(F)$ où F est le polynôme qui définit l'équation implicite de S.

$I_2 := I \cap \mathbb{C}[x,y,z]$ est donc de la forme :

$$I_2 = \langle F^k \rangle \text{ avec } k > 0$$

Le calcul de l'équation implicite de S se ramène donc au calcul d'une base de Gröbner de I.
(voir remarque2 p.12)

Exemple 1 : considérons la paramétrisation de la sphère unité :

$$(s,t) \quad \mapsto \quad (\frac{1-s^2-t^2}{1+s^2+t^2}, \frac{2s}{1+s^2+t^2}, \frac{2t}{1+s^2+t^2})$$

Une base de Gröbner pour l'ordre lexicographique $s > t > x > y > z$ de l'idéal

$$\langle 1 - s^2 - t^2 - x(1 + s^2 + t^2), 2s - y(1 + s^2 + t^2), 2t - z(1 + s^2 + t^2) \rangle$$

est

$$B = \{x^2 + y^2 + z^2 - 1, xz - z + y^2t + z^2t, -z + xt + t, zs - yt, ys + zt + x - 1, xs - y + s\},$$

et on a :

$$B \cap \mathbb{C}[x,y,z] = \{x^2 + y^2 + z^2 - 1\}.$$

On retrouve bien l'équation implicite classique de la sphère.

Exemple 2 : considérons une autre paramétrisation de la sphère unité :

$$(s,t) \quad \mapsto \quad (\frac{s^2-1-t^2}{1+s^2+t^2}, \frac{2s}{1+s^2+t^2}, \frac{2st}{1+s^2+t^2})$$

Une base de Gröbner pour l'ordre lexicographique $s > t > x > y > z$ de l'idéal

$$\langle s^2 - 1 - t^2 - x(1 + s^2 + t^2), 2s - y(1 + s^2 + t^2), 2st - z(1 + s^2 + t^2) \rangle$$

est

$$B' = \{y^2 + y^2t^2 + x^2 + x^2t^2 + z^2 + z^2t^2 - 1 - t^2, -z - zt^2 + yt + yt^3,$$
$$z^2s - yx - xyt^2 + sy^2 - y - yt^2, xs + y + yt^2 - s, -x - xt^2 + sy - 1 - t^2 + zst,$$
$$-zs + yst, -2st + z + zs^2 + zt^2, -2s + y + s^2y + yt^2\}$$

Cette fois on a :

$$B' \cap \mathbb{C}[x,y,z] = \phi$$

Dans le deuxième exemple la méthode échoue. Que s'est-il passé?
L'efficacité de la méthode n'a été démontrée que dans le cas sans point base dans le domaine affine. Que se passe-t-il si cette hypothèse n'est plus vérifiée? Supposons que les p_1,p_2,p_3,p_4 admettent une solution commune (s_0,t_0) dans $\mathbb{C}^2$.
Alors, avec les notations précédentes,

$$\forall (x,y,z) \in \mathbb{C}^3, \quad \begin{aligned} H_1(s_0,t_0,x,y,z) &= 0 \\ H_2(s_0,t_0,x,y,z) &= 0 \\ H_3(s_0,t_0,x,y,z) &= 0 \end{aligned}$$

donc $(s_0,t_0) \times \mathbb{C}^3 \subset Z$.
On a alors $\pi_2(Z) = \mathbb{C}^3$, et non plus comme avant $\pi_2(Z) = Im\varphi$.
Par conséquent $V(I_2) = \overline{\pi_2(Z)} = \mathbb{C}^3$, d'où $I_2 = \langle 0 \rangle$
On comprend donc pourquoi la méthode a échouée dans la deuxième exemple (car la paramétrisation admet le point $(0,i)$ comme point base).

Cette méthode, tout comme celle présentée au paragraphe précédent à base de résultants, échoue donc en présence de points bases. Cependant seuls les points bases *du domaine affine* sont pris en compte, ce qui est un avantage :
par exemple dans l'exemple 1, $(1,i,0)$ et $(1,-i,0)$ sont deux points bases à l'infini. Le calcul de I_2 a toutefois bien donné l'équation implicite de la sphère, alors que le calcul du résultant de H_1,H_2,H_3 aurait donné le polynôme nul.

On pourrait donc penser que les bases de Gröbner sont un outil plus satisfaisant que les résultants. C'est théoriquement vrai, mais en pratique un calcul de base de Gröbner, et particulièrement un calcul de base de Gröbner pour l'ordre lexicographique, est extrêmement coûteux (complexité doublement exponentielle [MeyMay88]).

4 Inversion et implicitisation

Nous allons maintenant présenter une méthode d'implicitisation des surfaces applicable dans le cas où celles-ci sont données par des paramétrisations propres. La méthode va toutefois nécessiter la connaissance de l'inverse de la paramétrisation (car toute paramétrisation propre est birationnelle, donc inversible), c'est pourquoi nous commencerons par donner un algorithme d'inversion des paramétrisations propres.

4.1 Un algorithme d'inversion

Le problème de l'inversion de la paramétrisation (propre) d'une surface est un problème qui reste encore assez ouvert actuellement, et pour lequel on ne dispose pas de beaucoup de méthodes (et encore moins de méthodes très efficaces) :
Donnons-nous une paramétrisation propre d'une surface S :

$$(s,t) \mapsto (\frac{p_1(s,t)}{p_0(s,t)}, \frac{p_2(s,t)}{p_0(s,t)}, \frac{p_3(s,t)}{p_0(s,t)})$$

• une première méthode consisterait à écrire la matrice de Dixon associée aux polynômes $p_0x_1 - p_1, p_0x_2 - p_2, p_0x_3 - p_3$ (cf. section 3.1), puis à utiliser la règle de Cramer pour dire que le quotient des mineurs de cette matrice correspondants à s^it^j et $s^{i-1}t^j$ (ou à s^it^j et s^it^{j-1}) fournit $s = \frac{s^it^j}{s^{i-1}t^j}$ (et $t = \frac{s^it^j}{s^it^{j-1}}$) en fonction de x_1, x_2, x_3. Cependant en présence de points bases la méthode échoue.
• Une autre méthode consisterait à calculer une base de Gröbner de l'idéal $\langle p_0x_1 - p_1, p_0x_2 - p_2, p_0x_3 - p_3, 1 - p_0w \rangle$ pour l'ordre lexicographique $s > t > w > x_1 > x_2 > x_3$ (voir le chapitre 6 au sujet de l'intérêt de rajouter le polynôme $1 - p_0w$); on sait alors qu'une telle base contient 2 polynômes linéaires en s et en t qui fournissent l'inverse de la paramétrisation. Toutefois le calcul de cette base de Gröbner est extrêmement coûteux.

S. Pérez. Diaz, J. Schicho et J.R. Sendra proposèrent très récemment un nouvel algorithme permettant de déterminer si une paramétrisation est propre ou non, et qui dans le cas positif donne l'inverse. Ses avantages sont de marcher même en présence de points bases, et d'être beaucoup plus rapide que la méthode utilisant les bases de Gröbner. La démonstration de son exactitude étant longue et sans rapport direct avec notre propos (l'implicitisation), nous renvoyons à [PDSS] pour la preuve. Les auteurs considèrent une paramétrisation dont la forme est un peu plus générale que celle que l'on utilise d'habitude :

$$\varphi : (s,t) \mapsto (\frac{p_1(s,t)}{q_1(s,t)}, \frac{p_2(s,t)}{q_2(s,t)}, \frac{p_3(s,t)}{q_3(s,t)})$$

(on impose pas que les dénominateurs soient égaux).
On note V la variété ainsi obtenue. Voici la description de cet algorithme :

• **Entrée** : les trois fractions rationnelles $\frac{p_1(s,t)}{q_1(s,t)}, \frac{p_2(s,t)}{q_2(s,t)}$ et $\frac{p_3(s,t)}{q_3(s,t)}$.

• **Sortie** : l'inverse de φ ou le message "φ *n'est pas propre*".

1) Définir :

$$\begin{aligned} H_1(s,t) &= x_1 q_1(s,t) - p_1(s,t) \\ H_2(s,t) &= x_2 q_2(s,t) - p_2(s,t) \\ H_3(s,t) &= x_3 q_3(s,t) - p_3(s,t). \end{aligned}$$

H_1,H_2 et H_3 sont vus comme des polynômes de $\mathbb{C}(V)[s,t]$, où $\mathbb{C}(V)$ désigne le corps des fractions ration-elles sur la variété V.

2) Vérifier que les PGCD des coefficients de tête de H_1,H_2,H_3 vus comme des polynômes en t à coefficients dans $\mathbb{C}(V)[s]$, pris deux à deux, soient égaux à 1. De même vérifier que les PGCD des coefficients de tête de H_1,H_2,H_3 vus comme des polynômes en s à coefficients dans $\mathbb{C}(V)[t]$, pris deux à deux, soient égaux à 1. Si ce n'est pas le cas, s'y ramener par un changement de coordonnées convenable).

3) On introduit une nouvelle variable Z.
Calculer $S(s) \in \mathbb{C}(V)[s]$ le contenu par rapport à Z du résultant par rapport à t des 2 polynômes H_1 et $H_2 + ZH_3$:

$$S(s) := cont_Z(res(H_1, H_2 + ZH_3, t)) \in \mathbb{C}(V)[s].$$

(On montre que les racines de $S(s)$ correspondent aux s-coordonnées des points d'intersection entre H_1,H_2 et H_3 dans $\mathbb{C}(V)^2$. La paramétrisation est propre **ssi** cette intersection ne contient qu'un seul point de $\mathbb{C}(V)^2 - \mathbb{C}$, ce point correspondant alors à l'inverse de la paramétrisation).

4) Calculer le polynôme $\overline{S(s)}$ obtenu à partir de $S(s)$ en éliminant les facteurs correspondant à des racines constantes.
(procéder comme ceci : on introduit deux nouvelles variables u et v et on remplace les

variables x,y,z dans $S(s)$ par $\frac{p_1(u,v)}{q_1(u,v)},\frac{p_2(u,v)}{q_2(u,v)},\frac{p_3(u,v)}{q_3(u,v)}$. Puis on élimine les dénominateurs en multipliant par un polynôme adéquat de $\mathbb{C}[u,v]$: le contenu de ce polynôme par rapport à u et v est un polynôme $C(s)$ de $\mathbb{C}[s]$ qui correspond aux racines constantes de $S(s)$.
Donc $\overline{S(s)} = S(s)/C(s)$.

5) Si $\overline{S(s)}$ est de degré 1 en s on pose α son unique racine. Sinon on renvoie le message "φ *n'est pas propre*".
(cf. la remarque entre parenthèses de l'étape 3)).

Les étapes 6),7) et 8) sont les analogues de 3),4), et 5) pour la coordonnée t :
6) Calculer $T(t) = cont_Z(res(H_1,H_2 + ZH_3,s)) \in \mathbb{C}(V)[t]$.

7) Calculer le polynôme $\overline{T(t)}$ obtenu à partir de $T(t)$ en éliminant les facteurs correspondant à des racines constantes.

8) Si $\overline{T(t)}$ est de degré 1 en t on pose β son unique racine. Sinon on renvoie le message "φ *n'est pas propre*".

9) On renvoie (α,β).

remarque: on ne connaît pas a priori l'équation implicite de V (puisque justement on veut appliquer cet algorithme au problème d'implicitisation!) : pour savoir si un polynôme $P(x_1,x_2,x_3)$ est nul dans $\mathbb{C}(V)$ il suffit alors de vérifier si $P(\frac{p_1(s,t)}{q_1(s,t)},\frac{p_2(s,t)}{q_2(s,t)},\frac{p_3(s,t)}{q_3(s,t)})$ est nul dans $\mathbb{C}(s,t)$. Cette substitution pouvant toutefois s'avérer coûteuse, pour vérifier si $P(x_1,x_2,x_3)$ est nul dans $\mathbb{C}(V)$ on se contente de vérifier que pour un point (s_0,t_0) tiré au hasard on a bien $P(\frac{p_1(s_0,t_0)}{q_1(s_0,t_0)},\frac{p_2(s_0,t_0)}{q_2(s_0,t_0)},\frac{p_3(s_0,t_0)}{q_3(s_0,t_0)}) = 0$.

Le code MAPLE de S. Pérez. Diaz, J. Schicho et J.R. Sendra de cet algorithme est donné en annexe; les variables à utiliser pour entrer les fractions rationnelles de la paramétrisation ne sont pas (s,t) mais $(t1,t2)$.

4.2 Application à l'implicitisation

Maintenant que nous disposons d'un algorithme d'inversion, nous allons pouvoir présenter la méthode très récente de I. Emiris et de J. R. Sendra (début 2002, non-

publié à ce jour) qui permet de résoudre le problème d'implicitisation lorsque la paramétrisation est propre et que l'on en connaît l'inverse.
On préserve les notations du paragraphe précédent :
φ est la paramétrisation propre d'une surface V, $F = 0$ est l'équation implicite de celle-ci, et M est l'inverse de φ (défini sur un ouvert de V). M est de la forme

$$M(x) = (\frac{A_1(x)}{B_1(x)}, \frac{A_2(x)}{B_2(x)}),$$

avec $x = (x_1,x_2,x_3)$, $B_i \neq 0$ dans $\mathbb{C}(V)$ et $PGCD(A_i,B_i) = 1$.
On note $Q = (Q_1,Q_2,Q_3)$ la composée

$$Q = \varphi \circ M \qquad \text{avec } Q_i \in \mathbb{C}(x_1,x_2,x_3)$$

(pour faciliter les notations on écrit de la même façon un élément de $\mathbb{C}[x_1,x_2,x_3]$ et sa classe d'équivalence dans $\mathbb{C}(V)$).
On suppose que les fractions rationnelles Q_i sont réduites,
ie que $PGCD(num(Q_i),denom(Q_i)) = 1$ (où $num(Q_i)$ désigne le numérateur de Q_i, et $denom(Q_i)$ son dénominateur).
Comme M est l'inverse de φ on a

$$\varphi \circ M(x) = x \ mod \ F$$

pour presque tout $x = (x_1,x_2,x_3) \in V$,

$$\textbf{ie} \quad Q_i = x_i \ mod \ F \quad i = 1,2,3.$$

On note $r \in \{0,1,2,3\}$ le nombre de Q_i qui sont exactement égaux à x_i.

Lemme 1 : $r \neq 3$.

Preuve :
Supposons $r = 3$, alors $\begin{cases} Q_1(x) = x_1 \\ Q_2(x) = x_2 \\ Q_3(x) = x_3 \end{cases}$, donc $\varphi \circ M(x_1,x_2,x_3) = (x_1,x_2,x_3)$ dans $\mathbb{C}(x_1,x_2,x_3)$.
Ceci implique que la fermeture de Zariski de $im(\varphi \circ M)$ dans $\mathbb{C}^3$ soit $\mathbb{C}^3$. Or la fermeture de Zariski de $im(\varphi)$ dans $\mathbb{C}^3$ est V, d'où une contradiction (car $\mathbb{C}^3 \not\subset V$).

On peut supposer sans perte de généralité que se sont les r premiers Q_i qui sont

égaux à x_i (dans $\mathbb{C}(x)$).

Lemme 2 : *1) Pour chaque $j \in \{r+1,\ldots,3\}$ il existe $l_j \in \mathbb{N}, l_j > 0$ et $H_j \in \mathbb{C}[x]$ tels que $num(Q_j - x_j) = F^{l_j} H_j$ et $PGCD(F,H_j) = 1$.*

2) $PGCD(H_{r+1},\ldots,H_3)$ est soit égal à 1, soit égal à un produit de facteurs appartenant soit à B_1, soit à B_2.

Preuve :

• Le premier point est évident.
• Observons ensuite que de la relation $num(Q_j) = x_j denom(Q_j) + F^{l_j} H_j$ on déduit que $PGCD(H_j,denom(Q_j)) = 1$ (sinon on contredit le fait que les Q_i ont été choisis réduits).
• Supposons que $H := PGCD(H_{r+1},\ldots,H_3) \neq 1$, et soit K un de ses facteurs irréductibles non-constant.
Supposons (absurde!) que K ne soit pas un facteur de B_1 ou de B_2. On note W la variété définie par K. On a alors que pour presque tout $P \in W$, l'expression $M(P)$ est bien définie, ainsi que l'expression $\varphi \circ M(P)$ (d'après le point précédent). De plus par définition de H, et comme K divise H, on a pour presque tout $P \in W$ $\varphi \circ M(P) = P$. De plus $\varphi \circ M(P) \in V$, donc $W \subset V$, ce qui contredit $PGCD(F,K) = 1$.

Lemme 3 : *Si $r = 2$, alors V peut-être paramétrée proprement par*

$$\varphi'(s,t) \mapsto (s,t,Q_3(s,t,a)),$$

où a est n'importe quel élément de $\mathbb{C}$ tel que $x_3 - a$ ne divise pas ni B_1, ni B_2, ni le dénominateur de Q_3.
(et $num(x_3 - Q_3(x_1,x_2,a)) = 0$ sera alors l'équation implicite de la surface)
Preuve :

On note $\overline{E}$ la fermeture de Zariski d'un ensemble E, $dim(E)$ sa dimension.
Soit a comme dans l'énoncé du lemme.
On peut alors définir

$$M' = \begin{pmatrix} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ (s,t) & \mapsto & M(s,t,a) \end{pmatrix}$$

On pose

$$\varphi' = \varphi \circ M'$$
$$\varphi'(s,t) = (s,t,Q_3(s,t,a)).$$

On a alors :
• pour presque tout $(s,t) \in \mathbb{C}^2$, $\varphi'(s,t) \in V$ (car $im\varphi \subset V$)
• $dim(\overline{im\varphi'}) \geq 2$ (c'est clair d'après la forme de φ').
• Des deux points précédents on déduit, comme V est irréductible, que $\overline{im\varphi'} = V$.
• Reste à voir que φ' est propre, **ie** birationnelle, mais c'est évident car φ et M le sont.

Des trois lemmes précédents, et sous la condition que l'on connaisse l'inverse M de φ (sinon on peut utiliser l'algorithme de paragraphe précédent pour calculer M), on déduit l'algorithme suivant d'implicitisation :

0) Calculer l'inverse M s'il n'est pas connu à l'avance.

1) Calculer $Q = \varphi \circ M$.

2) Si $r = 2$: supposons par exemple que $Q_3 \neq x_3$. Alors, d'après le lemme 3, l'équation implicite est donnée par

$$num(x_3 - Q_3(x_1,x_2,a)) = 0$$

où a est n'importe quel élément de $\mathbb{C}$ tel que $x_3 - a$ ne divise pas les dénominateurs de $M(x)$ ni celui de Q_3.

3) Si $r = 1$: supposons par exemple que $Q_1 = x_1$.
Alors posons $G(x) = squarefree(PGCD(num(Q_2 - x_2),num(Q_3 - x_3)))$.
L'équation implicite est donnée par (cf. lemme 2)

$$\frac{G(x)}{PGCD(G,B_1B_2)}.$$

4) Si $r = 0$: posons
$G(x) = squarefree(PGCD(num(Q_2 - x_2),num(Q_3 - x_3),num(Q_3 - x_3)))$.
L'équation implicite est alors donnée par (cf. lemme 2)

$$\frac{G(x)}{PGCD(G,B_1B_2)}.$$

Ceci est l'algorithme d'implicitisation proposé par I. Emiris et R. Sendra (à l'exception de l'étape 0, car les deux auteurs supposaient l'inverse connu d'avance).
Cet algorithme présente l'avantage de marcher même en présence de points bases, et de fournir directement l'équation implicite (plutôt qu'un multiple de celle-ci, contrairement à de nombreuses méthodes [cf. par ex les prochains chapitres]). Un autre avantage est qu'il peut se généraliser sans difficulté aux hypersurfaces.
Seulement il a de grosses faiblesses :
• D'abord supposer l'inverse connu est une hypothèse très forte, et calculer l'inverse est en général une opération très coûteuse qui a elle-seule peut suffire à dissuader d'employer la méthode. Par exemple dans l'exemple 5 (voir section 10) il faut 462s pour seulement calculer l'inverse de la paramétrisation, alors que d'autres méthodes testées trouvent l'équation implicite de la surface en moins d'une seconde; dans l'exemple 3 neuf heures ne suffisent pas à inverser une paramétrisation de degré 4, alors que l'équation implicite associée à cette paramétrisation est trouvée en moins de deux minutes pour la méthode ASSIA (cf plus loin).
• Ensuite pour appliquer l'algorithme, excepté lorsque $r = 2$, il faut calculer plusieurs PGCD (même l'opération *squarefree* est un PGCD déguisé) : or un calcul de PGCD pour des polynômes à plusieurs variables est aussi relativement coûteux.
• Enfin même le calcul $Q = \varphi \circ M$ est loin d'être négligeable, car cette substitution fait intervenir des polynômes de très haut degré, et il faut de plus réduire les fractions rationnelles Q_1,Q_2,Q_3 que l'on obtient. Dans l'exemple 4, le simple calcul de la première composante réduite Q_1 de Q prends 141s, contre "seulement 69s" pour calculer l'inverse M.

C'est pour pallier à ces deux derniers inconvénients que nous proposons une autre approche pour calculer l'équation implicite connaissant l'inverse M. Cette approche est certes plus simpliste, mais elle est concrètement plus efficace.
Cela consiste à appliquer l'algorithme suivant :

input : la paramétrisation et son inverse, **ie** φ et M.

output : l'équation implicite de la surface paramétrée.

1) Calculer Q_1.

2) Si $Q_1 \neq x_1$, alors $num(x_1 - Q_1)$ est un multiple non-nul de l'équation impli-

cite. Le factoriser, puis déterminer le facteur irréductible qui correspond à l'équation implicite.

3) Si $Q_1 = x_1$, reprendre les étapes 1) et 2) avec Q_2, puis avec Q_3 si nécessaire.

Le lemme 1 nous assure que l'algorithme marche.
Pour déterminer lequel des facteurs irréductibles correspond à l'équation implicite, on pourrait substituer dans chacun de ceux-ci les variables x_1,x_2,x_3 par Q_1,Q_2 et Q_3, et chercher lequel des facteurs correspond au polynôme nul : mais cela pourrait prendre beaucoup trop de temps. Connaissant la paramétrisation il est nettement plus rapide de choisir un point quelconque sur la surface, et avec probabilité presque égal à 1 l'équation implicite correspondra au seul facteur s'annulant en ce point.

Cet algorithme a deux gros avantages sur son prédécesseur :
• D'abord on est pas obligé de calculer Q_1,Q_2 et Q_3 : la plupart du temps connaître Q_1 suffit. Ce détail n'est pas négligeable : par exemple dans l'exemple 4 du chapitre 10 il faut 69s pour calculer l'inverse de la paramétrisation, 141s pour calculer Q_1 et 22s pour factoriser $num(x_1 - Q_1)$. Dans ce cas le calcul de Q_1 est de loin l'étape qui prend le plus de temps, d'où l'intérêt d'éviter le calcul de toutes les composantes de Q.
• Ensuite on ne calcule qu'une seule factorisation par cette méthode, contre plusieurs PGCD pour l'autre algorithme : or calculer un PGCD pour des polynômes à plusieurs variables n'est pas vraiment plus facile que de factoriser. D'autant plus que MAPLE est particulièrement efficace pour la factorisation.

Les exemples traités au chapitre 10 tendent à montrer que le deuxième algorithme est beaucoup plus efficace que celui proposé par I. Emiris et R. Sendra. L'exemple 4 est à ce sujet assez significatif.

5 La méthode d'Ariès-Senoussi

Soit S une surface de $\mathbb{C}^3$ paramétrée par

$$\varphi = \left(\begin{array}{ccc} \mathbb{P}^2 & \longrightarrow & \mathbb{C}^3 \\ (s:t:u) & \mapsto & (\frac{p_1(s:t:u)}{p_4(s:t:u)}, \frac{p_2(s:t:u)}{p_4(s:t:u)}, \frac{p_3(s:t:u)}{p_4(s:t:u)}) \end{array} \right)$$

où les p_i sont quatre polynômes de degré total n. On suppose dans tout ce chapitre φ *sans point base*. On a vu au paragraphe 3.1 que l'équation implicite de S était donnée par le résultant de $p_1 - xp_4, p_2 - yp_4, p_3 - zp_4$. Par ailleurs, on a vu que le résultant de trois polynômes f,g,h homogènes **génériques** de degré total d est de degré total $3d^2$ en les coefficients de ces polynômes. Or **dans le cas particulier** où $f = p_1 - xp_4, g = p_2 - yp_4, h = p_3 - zp_4$ on sait que Res(f,g,h) est un polynôme en x,y,z de degré seulement d^2. Autrement dit pour calculer $Res_{p_1-xp_4,p_2-yp_4,p_3-zp_4}$ on manipule des monômes qui sont de degré nettement supérieurs à ceux dont on a *réellement* besoin.
C'est pour pallier à ce défaut (qui a pour conséquence des calculs alourdis) que Frank Aries et Rachid Senoussi proposèrent en 2001 un nouvel algorithme d'implicitisation des surfaces [AR].
L'idée est de mettre au point non pas un algorithme permettant de calculer le résultant de trois polynômes génériques (car on a pas besoin d'un algorithme aussi général), mais un algorithme plus adapté au problème du calcul du résultant de polynômes de type $(p_1 - xp_4, p_2 - yp_4, p_3 - zp_4)$. Aries et Senoussi ont appelé leur algorithme ASSIA, pour "Adapted Sylvester Surface Implicitization Algorithm". Celui-ci est en effet inspiré de l'algorithme mis au point par Sylvester en 1852 pour calculer le résultant de 3 polynômes de même degré.

Pour présenter l'algorithme ASSIA nous allons légèrement changer nos notations habituelles, et plonger la surface dans l'espace projectif (pour alléger les écritures) :
Soit $F_n = \{q = (q_1,q_2,q_3) \in \mathbb{N}^3 / q_1 + q_2 + q_3 = n\}$ $\quad \#F_n = \binom{n+2}{n}$
On pose :
$t := (t_1,t_2,t_3)$
$x := (x_1,x_2,x_3,x_4)$
$t^q := t_1^{q_1} t_2^{q_2} t_3^{q_3}$ pour $q \in F_n$
S est donc maintenant une surface de $\mathbb{P}^3$ paramétrée par

$$\varphi = \left(\begin{array}{ccc} \mathbb{P}^2 & \longrightarrow & \mathbb{P}^3 \\ (t_1:t_2:t_3) & \mapsto & (x_1 = p_1(t) : x_2 = p_2(t) : x_3 = p_3(t) : x_4 = p_4(t)) \end{array} \right)$$

avec $p_i(t) = \sum_{q \in F_n} \pi_{(i,q)} t^q, \qquad \pi_{(i,q)} \in \mathbb{C} \qquad i = 1,2,3,4$
On note π l'ensemble des coefficients $\pi_{(i,q)}$.

Description de l'algorithme ASSIA :

Etape 1 : on considère une quatrième variable λ et on pose

$$Q_i(t,\lambda) := p_i(t) - x_i \lambda^n$$

Puis on multiplie les Q_i par tous les monômes $x^q, q \in F_{n-2}$, pour obtenir $m_1 = 4\binom{n}{2}$ polynômes homogènes de degré $2n-2$ en (t,λ) :

$$t^q Q_i(t,\lambda) = \sum_{j \in F_{2n-2}} a_{i,q,j}(\pi) t^j - x_i t^q \lambda^n$$

Etape 2 : pour chaque multi-index $\alpha \in F_{n-1}$ on écrit les Q_i sous la forme (écriture non unique) :

$$Q_i(t,\lambda) := A^1_{i,\alpha}(\pi,t) t_1^{\alpha_1+1} + A^2_{i,\alpha}(\pi,t) t_2^{\alpha_2+1} + A^3_{i,\alpha}(\pi,t) t_3^{\alpha_3+1} - x_i \lambda^n$$

et on calcule le déterminant $D_\alpha(t)$:

$$D_\alpha(t) = \begin{vmatrix} A^1_{1,\alpha}(\pi,t) & A^2_{1,\alpha}(\pi,t) & A^3_{1,\alpha}(\pi,t) & x_1 \\ A^1_{2,\alpha}(\pi,t) & A^2_{2,\alpha}(\pi,t) & A^3_{2,\alpha}(\pi,t) & x_2 \\ A^1_{3,\alpha}(\pi,t) & A^2_{3,\alpha}(\pi,t) & A^3_{3,\alpha}(\pi,t) & x_3 \\ A^1_{4,\alpha}(\pi,t) & A^2_{4,\alpha}(\pi,t) & A^3_{4,\alpha}(\pi,t) & x_4 \end{vmatrix}$$
$$= \sum_{j \in F_{2n-2}} b_{\alpha,j}(\pi,x) t^j$$

Remarques :
• Si pour une spécialisation (π_0,x_0), les Q_i ont une solution (t_0,λ_0), alors $D_\alpha(t_0) = 0$ $\forall \alpha$.
• On obtient ainsi $m_2 = \binom{n+1}{2}$ polynômes $D_\alpha(t)$ de degré $2n-2$ en t car $n - (\alpha_1 + 1) + n - (\alpha_2 + 1) + n - (\alpha_3 + 1) = 2n - 2$.
• Les $b_{\alpha,j}(\pi,x)$ sont des polynômes homogènes de $\mathbb{Z}[\pi,x]$ de degré 4, linéaires en x et de degré 3 en π.

Etape 3 : on a donc construit $m_1 + m_2 = 2n(n-1) + \frac{n(n+1)}{2} = \frac{(5n-3)n}{2}$ polynômes :

$$\begin{array}{rcl} t^q Q_i(t,\lambda) & = & \sum_{j\in F_{2n-2}} a_{i,q,j}(\pi)t^j \quad + \quad \sum_{s\in F_{n-2}} x_i\delta_{s,q}(t^s\lambda^n) \\ D_\alpha(t) & = & = \sum_{j\in F_{2n-2}} b_{\alpha,j}(\pi,x)t^j \quad + \quad \sum_{s\in F_{n-2}} 0\times(t^s\lambda^n) \end{array}$$

où $\delta_{s,q}$ vaut 1 si $s=q$, 0 sinon.
Ces polynômes sont déterminés par $\binom{2n}{2}+\binom{n}{2}=\frac{(5n-3)n}{2}$ coefficients.
On range tous ces coefficients dans une matrice carrée de taille $\frac{(5n-3)n}{2}$:

$$M(\pi,x)=\begin{pmatrix} a_{i,q,j}(\pi) & , & x_i\delta_{s,q} \\ b_{i,q,j}(\pi) & , & 0 \end{pmatrix},$$

Posons $m(\pi,x)=det(M(\pi,x))$.

Soit $R(\pi,x_1,x_2,x_3)$ le résultant de $p_1-x_1p_4,p_2-x_1p_4,p_3-x_1p_4$.
Comme pour présenter l'algorithme ASSIA on a adopté les notations homogènes par rapport à x, il nous faut considérer le polynôme obtenu par homogénéisation de $R(\pi,x_1,x_2,x_3)$, et que l'on notera $R^h(\pi,x_1,x_2,x_3,x_4)=R^h(\pi,x)$. (**ie** R et R^h ont même degré et $R^h(\pi,x_1,x_2,x_3,1)=R^h(\pi,x_1,x_2,x_3)$
On a le résultat annoncé en début de section :

Théorème 5.1 $m(\pi,x)=R^h(\pi,x)$.

Preuve :

Admettons temporairement que $R^h(\pi,x)$ soit irréductible comme polynôme de $\mathbb{C}[\pi,x]$.
• $m(\pi,x)$ n'est pas le polynôme nul car pour $p_i(x)=x_i^n$ $i=1,2,3$ et $p_4(x)=(x_1^n+x_2^n+x_3^n)$ on a

$$m(\pi,x)=(x_4-x_3-x_2-x_1)^{r^2}$$

• Par construction $m(\pi,x)$ est un polynôme de degré $3\binom{2+(n-1)}{2}+(4\binom{2+(n-2)}{2}-\binom{2+(n-2)}{2})=3n^2$ en π et de degré $\binom{2+(n-2)}{2}+\binom{2+(n-1)}{2}=n^2$ en x.
• De plus, toujours par construction, m s'annule pour une spécialisation (π_0,x_0) lorsque R^h s'annule pour cette même spécialisation et que la paramétrisation associée à π_0 n'a pas de point base.
Donc, comme R^h est irréductible, on en déduit que $R^h(\pi,x)$ divise $m(\pi,x)$, et comme R^h et m ont même degré en π et en x on conclut que

$$\boxed{R^h(\pi,x)=m(\pi,x).}$$

• Reste à voir pour être complet que $R^h(\pi,x)$ est irréductible dans $\mathbb{C}[\pi,x]$
(Ceci ne peut pas simplement se déduire du fait que le résultant de trois polynômes génériques de degré n soit irréductible).
Considérons le système

$$\begin{cases} Q_1(t,\lambda) := p_1(t) - x_1\lambda^n \\ Q_2(t,\lambda) := p_2(t) - x_2\lambda^n \\ Q_3(t,\lambda) := p_3(t) - x_3\lambda^n \\ Q_4(t,\lambda) := p_4(t) - x_4\lambda^n \end{cases}$$

D'après le théorème d'existence des résultants énoncé à la section 3.1, il existe un polynôme $S(\pi,x) \in \mathbb{Z}[\pi,x]$, irréductible dans $\mathbb{C}[\pi,x]$, unique au signe près, qui s'annule pour une spécialisation (π_0,x_0) **ssi** le système correspondant admet une solution non-triviale.
Comme $S(\pi,x)$ est irréductible, pour montrer que $R^h(\pi,x)$ l'est il suffit de montrer que $R^h(\pi,x) = S(\pi,x)$.
Pour cela, déshomogénéisons S et montrons que $R(\pi,x_1,x_2,x_3) = S(\pi,x_1,x_2,x_3,1)$.
Supposons que R s'annule pour une spécialisation $(\overline{\pi},\overline{x_1},\overline{x_2},\overline{x_3})$ de (π,x_1,x_2,x_3).
Alors il existe $t_0 \in \mathbb{P}^2$ tel que

$$\begin{cases} p_1(t_0) = \overline{x_1}p_4(t_0) \\ p_2(t_0) = \overline{x_2}p_4(t_0) \\ p_3(t_0) = \overline{x_3}p_4(t_0) \end{cases}$$

Par conséquent le système

$$\begin{cases} p_1(t) - \overline{x_1}\lambda^n = 0 \\ p_2(t) - \overline{x_2}\lambda^n = 0 \\ p_3(t) - \overline{x_3}\lambda^n = 0 \\ p_4(t) - 1\lambda^n = 0 \end{cases}$$

admet la solution (t_0,α), où α est une solution de l'équation $p_4(t_0) = \alpha^n$.
Donc $S(\overline{\pi},\overline{x_1},\overline{x_2},\overline{x_3},1)$ s'annule, d'où $V(R(\pi,x_1,x_2,x_3)) \subset V(S(\pi,x_1,x_2,x_3,1))$.
Comme $S(\pi,x_1,x_2,x_3,1)$ est irréductible dans $\mathbb{C}[\pi,x_1,x_2,x_3]$ on en déduit que

$$R(\pi,x_1,x_2,x_3) = [S(\pi,x_1,x_2,x_3,1)]^\beta \text{ avec } \beta \in \mathbb{N} - 0.$$

Mais forcément $\beta = 1$ (car pour une spécialisation π_0 de π telle que la paramétrisation soit propre et sans point base on sait que $R(\pi_0,x_1,x_2,x_3)$ doit être *irréductible* et égal à l'équation implicite de la surface paramétrée).
CQFD

Cette méthode ne marche, comme on l'a dit, que si la paramétrisation est sans point base. Dans ce cas si on applique la procédure MAPLE de triangularisation *ffqausselim* à $M(\pi,x)$, l'équation implicite de la surface est donnée par l'unique élément non-nul de la dernière ligne de *ffqausselim*$M(\pi,x)$ (car cet élément correspond au déterminant de $M(\pi,x)$.
Franck Ariès et Rachid Senoussi ont cependant remarqué sur de nombreux exemples que lorsqu'il y a des points bases, tous les éléments de la dernière ligne non-nulle de la matrice *ffqausselim*$M(\pi,x)$ s'avèrent être des multiples de l'équation implicite. Toutefois une telle conjecture n'a pas encore pu être démontrée (pour retrouver l'équation implicite à partir d'un multiple de celle-ci il suffit alors de factoriser le multiple et de tester chacun de ses facteurs).

Exemple : considérons la paramétrisation suivante de la sphère unité :

$$\varphi : (t_1,t_2,t_3) \mapsto (\frac{t_3^2 - t_1^2 - t_2^2}{t_3^2 + t_1^2 + t_2^2}, \frac{2t_1t_3}{t_3^2 - t_1^2 - t_2^2}, \frac{2t_2t_3}{t_3^2 - t_1^2 - t_2^2}).$$

$(1,i,0)$ est un point base de la paramétrisation.
La procédure *ffqausselim* appliquée à $M(\pi,x)$ donne dans ce cas la matrice

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 1 & x \\ 0 & 0 & -2 & 0 & 0 & 0 & -y \\ 0 & 0 & 0 & 0 & -4 & 0 & -2z \\ 0 & 0 & 0 & 0 & 0 & -8 & -4w - 4x \\ 0 & 0 & 0 & 0 & 0 & 0 & -16y^2 - 16z^2 + 16w^2 - 16x^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Ici l'équation implicite est donnée directement par la dernière ligne non-nulle de cette matrice.

De toutes les méthodes testées dans ce document, ASSIA apparaît comme la plus puissante en général. Sa force vient du fait que l'équation implicite cherchée est donnée sous la forme d'un *unique* déterminant (pas de PGCD ou de quotient à calculer, ni de factorisation à effectuer comme pour de nombreuses autres méthodes) : pour trouver une équation implicite il suffit simplement de spécialiser des valeurs dans une matrice qui ne dépend que du degré total de la paramétrisation, et de calculer son déterminant.
Voir le chapitre 10 pour des exemples de calculs ainsi que leur rapidité.

6 Un nouvel algorithme utilisant les bases de Gröbner

Nous avons vu à la section 3.2 comment traiter le problème de l'implicitisation à l'aide des bases de Gröbner. Cette méthode présentait deux très grosses faiblesses : d'abord elle échouait automatiquement dès que la paramétrisation admettait des points bases dans le domaine affine, mais surtout elle reposait sur un calcul de base de Gröbner, qui plus est pour l'ordre lexicographique, ce qui est extrêmement coûteux. Par exemple la méthode d'Aries-Senoussi permet de trouver l'équation implicite de la surface paramétrée par

$$\varphi : (s,t) \mapsto (\tfrac{2s^3+13+st^2+7ts^2}{2t^2+s+19+4s^2t+7t+s^3}, \tfrac{2t^3+s^2+15+4s^2t+6t+s^3}{2t^2+s+19+4s^2t+7t+s^3}, \tfrac{2t^2+s+17+9s^2t+7t+s^2}{2t^2+s+19+4s^2t+7t+s^3}).$$

en 10.690s secondes, alors que plus d'une heure ne suffira pas à la méthode de la section 3.2 pour aboutir (voir ex2 du chapitre 10).
Les bases de grobner ne sont pas pour autant à rejeter, car elles peuvent être utilisées dans des algorithmes plus performants. C'est notamment le cas pour l'algorithme (non-publié à ce jour) proposé par Olivier Ruatta et Philippe Trébuchet, qui permet même de résoudre le problème d'implicitisation en présence de points bases, et que nous allons maintenant présenter.
Cet algorithme repose sur trois idées.
Soit S une surface de $\mathbb{C}^3$ paramétrée par

$$\varphi = \begin{pmatrix} \mathbb{C}^2 - W & \longrightarrow & \mathbb{C}^3 \\ (s,t) & \mapsto & (\frac{p_1(s,t)}{p_4(s,t)}, \frac{p_2(s,t)}{p_4(s,t)}, \frac{p_1(s,t)}{p_4(s,t)}) \end{pmatrix}$$

où $W = \{(s,t) \in \mathbb{C}^2 / p_4(s,) = 0\}$.

Première idée : "localiser"

Nous allons raisonner comme à la section 3.2, mais au lieu de considérer l'idéal

$$I = \langle xp_4(s,t) - p_1(s,t), yp_4(s,t) - p_2(s,t), zp_4(s,t) - p_3(s,t) \rangle$$
$$I \subset \mathbb{C}[s,t,x,y,z]$$

nous allons considérer l'idéal

$$J = \langle xp_4(s,t) - p_1(s,t), yp_4(s,t) - p_2(s,t), zp_4(s,t) - p_3(s,t), wp_4(s,t) - 1 \rangle$$
$$J \subset \mathbb{C}[s,t,w,x,y,z].$$

Le polynôme $wp_4(s,t) - 1$ a été rajouté aux trois premiers pour contraindre le dénominateur p_4 à ne pas s'annuler (c'est ce qu'on appelle la "localisation"). Ainsi

$$V(J) = \left\{(s,t,w,x,y,z) \in \mathbb{C}^6 / p_4(s,t) \neq 0, w = \frac{1}{p_4(s,t)} \right.$$
$$\left. x = \frac{p_1(s,t)}{p_4(s,t)}, y = \frac{p_2(s,t)}{p_4(s,t)}, z = \frac{p_3(s,t)}{p_4(s,t)} \right\}$$

On pose

$$\pi_3 = \begin{pmatrix} \mathbb{C}^6 & \longrightarrow & \mathbb{C}^3 \\ (s,t,w,x,y,z) & \mapsto & (x,y,z) \end{pmatrix}$$

et on a alors

$$\pi_{\mathbf{3}}(\mathbf{V}(\mathbf{J})) = \mathbf{Im}\varphi.$$

(C'est pour cela que le polynôme $wp_4(s,t) - 1$ a été rajouté à I, car en présence de points bases l'égalité-clé $\pi_2(V(I)) = Im\varphi$ de la section 3.2 ne reste plus valable.)
En prenant la clôture de Zariski de cette égalité on a :

$$\overline{\pi_3(V(J))} = \overline{Im\varphi} = S.$$

Or d'après le théorème rappelé au début de la section 3.2,

$$S = \overline{\pi_3(V(J))} = V(J \cap \mathbb{C}[x,y,z]),$$

donc l'idéal $J \cap \mathbb{C}[x,y,z]$ est de la forme

$$J \cap \mathbb{C}[x,y,z] = \langle F^k \rangle$$

où $F = 0$ est l'équation implicite irréductible de S, et k un entier ≥ 1.
(rappel : la remarque 2 page 12 explique comment retrouver F à partir de F^k).
Le calcul de l'équation implicite de S se ramène donc au calcul d'une base de Gröbner pour l'ordre lexicographique $s > t > w > x > y > z$ de l'idéal J.

Cette modification de la méthode de la section 3.2 permet maintenant la résolution théorique du problème d'implicitisation même en présence de points bases.
Mais en pratique il reste toujours le problème de la grande complexité du calcul d'une base de Gröbner, en particulier du calcul d'une base de Gröbner pour un ordre monomial lexicographique (de plus l'introduction d'une nouvelle variable w n'arrange rien).

Deuxième idée : changer l'ordre monomial

Il s'agit d'éviter le calcul d'une base de Gröbner pour l'ordre monomial lexicographique $s > t > w > x > y > z$ de l'idéal J.
L'algorithme suivant va nous permettre de retrouver l'équation implicite à partir d'une base de Gröbner de J pour un ordre monomial quelconque :

1) Calculer une base de Gröbner de J pour un ordre monomial **quelconque**.

2) Choisir un entier k inférieur ou égal à celui de l'équation implicite. L'idéal serait de choisir un entier k égal au degré de l'équation implicite (voir la section 2.2 à ce sujet), mais sinon il suffit de prendre $k = 1$.

3) Construire la liste L_k de tous les monômes de $\mathbb{C}[x,y,z]$ de degré inférieur ou égal à k.

4) Calculer le reste (unique) de la division de chaque monômes de L_k par la base de Gröbner de J du 1).
Tous les monômes faisant partie du support de ces restes forment une liste notée C_k.

5) Construire une matrice M_k à $\#L_k$ lignes et $\#C_k$ colonnes dont l'élément $M_k[i,j]$ correspond au coefficient du monômes $C_k[j]$ dans le reste de $L_k[i]$.

6) Si M_k est de rang maximal, reprendre à l'étape 3 avec k :=k+1; Si M_k n'est pas de rang maximal, alors le noyau de ${}^tM_k$ est de dimension 1, et un vecteur non-nul de ce noyau est formé des coefficients de l'équation implicite.

Pour prouver l'algorithme, la seule chose à dire est qu'un élément non-nul du noyau de ${}^tM_k$ correspond à une relation entre les monômes de L_k dans $\frac{\mathbb{C}[x,y,z]}{J}$, donc à un multiple de l'équation implicite;
Soit d le degré de l'équation implicite.
Si $k < d$, on a donc $ker(M_k) = ker({}^tM_k) = \{0\}$.
Si $k = d$, on a $dim(ker(M_k)) = dim(ker({}^tM_k)) = 1$, et $ker({}^tM_k)$ est engendré par les coefficients de l'équation implicite (car dans $\frac{\mathbb{C}[x,y,z]}{J}$, la seule relation entre des monômes de degré $\leq d$ est donnée par l'équation implicite).

On a donc vu dans ce paragraphe comment ramener le calcul du l'équation implicite de S (même avec points bases) au calcul d'une base de Gröbner de l'idéal $J \subset \mathbb{C}[s,t,w,x,y,z]$ pour *l'ordre monomial de notre choix.*
Toutefois le calcul d'une base de Gröbner, même pour un ordre non-lexicographique, reste très coûteux, notamment à cause de l'accroissement très rapide de la taille des coefficients des polynômes.
c'est pour pallier à cet inconvénient que l'on utilise une nouvelle amélioration.

Troisième idée : faire du calcul modulaire

Pour éviter l'exponentiation de la taille des coefficients lors du calcul de la base de Gröbner on va faire tous les calculs dans $\mathbb{Z}/p\mathbb{Z}$, avec p premier (car la méthode exposée jusque là reste applicable dans les corps finis).
(il est alors supposé implicitement que p_1,p_2,p_3,p_4 sont dans $\mathbb{Z}[s,t]$, ce qui est toujours le cas en CAO à partir du moment où on veut pouvoir faire du calcul exact.)
Évidemment l'algorithme décrit précédemment n'a alors aucune raison de donner exactement l'équation implicite mais, excepté pour un nombre fini de valeurs de p, on obtient un polynôme dont le support monomial est le même que celui de l'équation implicite cherchée.
Une étude détaillée des différentes étapes de l'algorithme précédent révèle que les valeurs de p à éviter sont les nombres premiers qui divisent :
a) les coefficients des monômes de têtes de la base de Gröbner calculée a l'étape 1) [pour que la base de Gröbner de J calculée dans $\mathbb{Z}/p\mathbb{Z}$ corresponde à la réduction modulo p de la base de Gröbner de J calculée dans $\mathbb{Q}$].
b) les termes diagonaux des matrices triangulaires $ffgausselim(M_k)$, $k = 1 \ldots d$, où d est le degré de l'équation implicite [pour que le rang des matrices M_k reste le même en calcul modulaire]
c) les coefficients de l'équation implicite cherchée.

Une fois le support de l'équation implicite connu, il est facile de retrouver celle-ci à l'aide de la prochaine proposition :
• Soit $E \subset \mathbb{N}^3$ tel que $\{m_\alpha = x^{\alpha_1} y^{\alpha_2} z^{\alpha_3} / \alpha = (\alpha 1,\alpha 2,\alpha 3) \in E\}$ soit le support mo-

nomial de l'équation implicite $F(x,y,z) = 0$, ie F est de la forme $F = \sum_{\alpha \in E} a_\alpha m_\alpha$.
• Soit $Z = \{\zeta_1, \ldots, \zeta_r\} \in S$ un ensemble de r points de la surface, $r = \#E$.

Proposition 6.1 *Si la matrice*

$$V_{E,Z} = \begin{pmatrix} m_{\alpha_1}(\zeta_1) & \cdots & m_{\alpha_r}(\zeta_1) \\ \vdots & \ddots & \vdots \\ m_{\alpha_1}(\zeta_r) & \cdots & m_{\alpha_r}(\zeta_r) \end{pmatrix}$$

est de rang $r-1$, alors le polynôme associé à un vecteur du noyau de $V_{E,Z}$ est l'équation implicite.

La proposition est évidente, car si F s'écrit $F = \sum_{\alpha \in E} a_\alpha m_\alpha$, alors le vecteur colonne dont les r coefficients sont les a_α est dans le noyau de la matrice.

Or pour un choix générique des points ζ_i, la matrice $V_{E,Z}$ est de rang r-1, donc à partir de la connaissance du support monomial de F il est possible facilement de retrouver F.

Nous disposons donc d'une nouvelle méthode d'implicitisation des surfaces qui s'effectue en deux étapes :

1) Trouver le support de l'équation implicite (en appliquant les deux premières idées mais en faisant tous les calculs modulo un entier p premier, avec p assez grand [par exemple $p = 32051$]).

2) Trouver l'équation implicite de la surface connaissant le support de celle-ci (en appliquant la troisième idée).

On obtient une méthode qui s'avère être très efficace lorsqu'on la teste sur des exemples (voir chapitre 10). De plus non seulement celle-ci marche en présence de points bases, mais la présence de points bases augmente sa rapidité : en effet les points bases font chuter le degré de l'équation implicite (voir paragraphe 3.2), donc le support de celle-ci est plus petit (voir les exemples 4,5 et 6 du chapitre 10).

7 Implicitisation et surfaces mobiles

7.1 Présentation du principe de la méthode

Toutes les méthodes d'implicitisation vues jusqu'à présent étaient soient à base de résultants, soit à base de bases de Gröbner. Nous allons maintenant présenter une toute autre approche du problème, basée sur une idée de Sederberg.
Soit une surface rationnelle S de $\mathbb{P}^3$ donnée par $(x(s,t) : y(s,t) : z(s,t) : w(s,t))$, où $(x(s,t),y(s,t),z(s,t),w(s,t))$ sont des polynômes en (s,t).
Note : Dans tout ce chapitre "$x(s,t)$" désignera un polynôme et "x" désignera simplement une variable (de même pour y,z,w).

Définition 7.1 *On appelle surface mobile une équation du type :*

$$g(x,y,z,w,s,t) = \sum_{i=1}^{\sigma} f_i(x,y,z,w)\gamma_i(s,t) = 0$$

où les équations $f_i(x,y,z,w) = 0$ définissent une collection de surfaces implicites et où les $\gamma_i(s,t)$ sont une collection de polynômes en s et t. Les $\gamma_i(s,t)$ sont supposés être linéairement indépendants et premiers dans leur ensemble.
Si tous les $f_i = 0$ correspondent à des plans on parle de plans mobiles
Si tous les $f_i = 0$ correspondent à des quadriques on parle de quadriques mobiles
On dit qu'une surface mobile suit la paramétrisation de S si on a :

$$g(x(s,t),y(s,t),z(s,t),w(s,t),s,t) \equiv 0$$

Une surface mobile est donc une famille de surfaces paramétrées par (s,t).
A chaque (s_0,t_0) on peut associer une surface $\sum_{i=1}^{\sigma} f_i(x,y,z,w)\gamma_i(s_0,t_0) = 0$ et un point $x(s_0,t_0),y(s_0,t_0),z(s_0,t_0),w(s_0,t_0)$ de S. Géométriquement, le fait qu'une surface mobile suive la paramétrisation de S veut dire que $x(s_0,t_0),y(s_0,t_0),z(s_0,t_0),w(s_0,t_0)$ est un point de $\sum_{i=1}^{\sigma} f_i(x,y,z,w)\gamma_i(s_0,t_0) = 0$, et ce pour tout (s_0,t_0).

Si on peut trouver un ensemble de σ surfaces mobiles

$$g_j(x,y,z,w,s,t) = \sum_{i=1}^{\sigma} f_{j,i}(x,y,z,w)\gamma_i(s,t) = 0 \quad j = 1..\sigma$$

qui suivent la paramétrisation, alors on peut construire une matrice carrée de taille $\sigma \times \sigma$:

$$M(x,y,z,w) = \begin{pmatrix} f_{1,1}(x,y,z,w) & \cdots & f_{1,\sigma}(x,y,z,w) \\ \vdots & \ddots & \vdots \\ f_{\sigma,1}(x,y,z,w) & \cdots & f_{\sigma,\sigma}(x,y,z,w) \end{pmatrix}$$

dont le déterminant $D(x,y,z,w)$ est un polynôme qui s'annule sur la surface S :
en effet, comme les γ_i n'ont pas de facteur commun (par hypothèse) il y a au plus un nombre fini de valeurs (s_0,t_0) telles que le vecteur $[\gamma_1(s_0,t_0),\ldots,\gamma_\sigma(s_0,t_0)]$ soit nul. $[\gamma_1(s_0,t_0),\ldots,\gamma_\sigma(s_0,t_0)]$ est donc un vecteur génériquement différent du vecteur nul qui vérifie de plus

$$M(x(s,t),y(s,t),z(s,t),w(s,t)) \begin{pmatrix} \gamma_1(s,t) \\ \vdots \\ \gamma_\sigma(s,t) \end{pmatrix} = 0$$

On en déduit que $D(x(s,t),y(s,t),z(s,t),w(s,t))$ est génériquement nul, donc nul (car c'est un polynôme).
D s'annule bien sur S.
Si de plus on a pu choisir les surfaces mobiles g_j telles que $D(x,y,z,w)$ ait le même degré que l'équation implicite (irréductible) de S, alors on en déduira que l'équation implicite de S est $D(x,y,z,w) = 0$.
On note au passage que la présence de points bases facilite l'application de cette méthode, puisque les points bases abaissent le degré de l'équation implicite, donc diminue la taille que doit avoir la matrice $M(x,y,z,w)$.

Exemple 1 :

$$\begin{aligned} x(s,t) &= st+1 \\ y(s,t) &= s \\ z(s,t) &= t \\ w(s,t) &= s+t+1 \end{aligned}$$

Le degré théorique de l'équation implicite de la surface est $2^2 - 2 = 2$ (car la paramétrisation est propre, de degré total 2, avec 2 points bases à l'infini qui sont $(1:0:0)$ et $(0:1:0)$).
On trouve facilement les deux surfaces mobiles suivantes :

$$(w-x-y-z)+sz = 0 \quad (11)$$

$$(w-x-2y-z)+s(w-y) = 0 \quad (12)$$

Le déterminant

$$\begin{vmatrix} (w-x-y-z) & z \\ (w-x-2y-z) & w-y \end{vmatrix} = w^2 - wx - 2wy + xy + y^2 - 2wx + xz + 3yz + z^2$$

fournit l'équation implicite de la surface.

Exemple2 :

$$\begin{aligned} x(s,t,u) &= st \\ y(s,t,u) &= u^2 \\ z(s,t,u) &= s^2 + tu \\ w(s,t,u) &= tu \end{aligned}$$

(on est passé en notations homogènes). Le degré théorique de l'équation implicite de la surface est $2^2 - 1 = 3$ (car la paramétrisation est propre, de degré total 2, avec un unique point base à l'infini qui est $(0:1:0)$).
On trouve facilement les trois surfaces mobiles suivantes :

$$uw - tw = 0 \quad (13)$$
$$sw - ux = 0 \quad (14)$$
$$tw - tz + sx = 0 \quad (15)$$

Le déterminant

$$\begin{vmatrix} w & 0 & -x \\ x & w-z & 0 \\ 0 & y & -w \end{vmatrix} = -w^3 + w^2 z - x^2 y$$

fournit l'équation implicite de la surface.

Dans les deux exemples, les surfaces mobiles étaient des plans mobiles.
Sur ces exemples on voit que la méthode des surfaces mobiles peut s'appliquer a priori même aux surfaces avec points bases.
Pour pouvoir appliquer la méthode des surfaces mobiles au problème de l'implicicitisation il nous faut répondre à deux questions :
1) A quelle(s) condition(s) existe-t-il des surfaces mobiles g_j qui suivent la paramétrisation et à partir desquelles on pourra former une matrice dont le déterminant

aura exactement le degré de l'équation implicite?
2) Si de telles surfaces mobiles existent, comment les trouver facilement?

Ces deux questions n'ont pas encore de réponses complètes à ce jour. Nous allons dans la suite présenter deux cas particuliers que l'on sait traiter :
- les paramétrisations de degré n sans point base.
- les paramétrisations de degré m en s et n en t sans point base (ie de bidegré (m,n)).

7.2 Cas des paramétrisations de bidegré (m,n) sans point base

On considère une paramétrisation d'une surface S de la forme :

$$\phi = \begin{pmatrix} \mathbb{C}^2 & \longrightarrow & \mathbb{P}^3 \\ (s,t) & \mapsto & (x(s,t) : y(s,t) : z(s,t) : w(s,t)) \end{pmatrix}$$

avec $x(s,t)$,$y(s,t)$,$z(s,t)$ et $w(s,t)$ quatre polynômes de bidegré (m,n) :

$$\begin{array}{ll} x(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} s^i t^j & y(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} s^i t^j \\ z(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} c_{i,j} s^i t^j & w(s,t) = \sum_{i=0}^{m} \sum_{j=0}^{n} d_{i,j} s^i t^j \end{array}$$

On suppose ϕ sans point base i.e. sans point base autre que les points bases canoniques à l'infini qui sont inhérents à ce type de paramétrisation [voir section 2.2]).
On appelle "plan mobile de bidegré (p,q)" une surface mobile de la forme :

$$A(s,t)x + B(s,t)y + C(s,t)z + D(s,t)w = 0$$

avec A,B,C,D des polynômes de bidegré (p,q).
On appelle "quadrique mobile de bidegré (p,q)" une surface mobile de la forme :

$$A(s,t)x^2 + B(s,t)xy + C(s,t)xz + \ldots + I(s,t)zw + J(s,t)w^2 = 0$$

avec A,B,C,$\ldots$,I,J polynômes de bidegré (p,q).
Dans toute la suite on ne considérera que des plans mobiles ou des quadriques mobiles de bidegré $(m-1,n-1)$.
On pose $R_{m,n} = \{P \in \mathbb{C}[s,t] / P \text{ de bidegré } (m,n)\}$
On définit :

$$MP = \begin{pmatrix} R^4_{m-1,n-1} & \longrightarrow & R_{2m-1,2n-1} \\ (A,B,C,D) & \mapsto & (A(s,t)x(s,t) + B(s,t)y(s,t) + C(s,t)z(s,t) + D(s,t)w(s,t)) \end{pmatrix}$$

$$MQ = \begin{pmatrix} R^{10}_{m-1,n-1} & \longrightarrow & R_{3m-1,3n-1} \\ (A,B,\ldots,I,J) & \mapsto & (A(s,t)x^2(s,t) + B(s,t)x(s,t)y(s,t) + \ldots \\ & & \ldots + I(s,t)z(s,t)w(s,t) + J(s,t)w^2(s,t)) \end{pmatrix}$$

Les plans mobiles de bidegré $(m-1,n-1)$ qui suivent la paramétrisation sont donnés par le noyau de MP.
Comme $dim(R^4_{m-1,n-1}) = dim(R_{2m-1,2n-1}) = 4mn$, si MP est de rang maximal il n'existe pas de plans mobiles de bidegré $(m-1,n-1)$ qui suivent ϕ.
Les quadriques mobiles de bidegré $(m-1,n-1)$ qui suivent la paramétrisation sont données par le noyau de MQ.
Comme $dim(R^{10}_{m-1,n-1}) = 10mn$ et $dim(R_{3m-1,3n-1}) = 9mn$, il existe au moins mn quadriques mobiles de bidegré $(m-1,n-1)$ qui suivent ϕ et qui sont linéairement indépendantes, avec égalité si MQ est de rang maximal.

Plaçons nous justement dans le cas où MQ est de rang maximal : on choisit alors $(Q_i)_{i=1\ldots mn}$ un ensemble de mn quadriques mobiles de bidegré $(m-1,n-1)$ qui suivent ϕ et qui sont linéairement indépendantes.
Chaque Q_i s'écrit :

$$\begin{aligned} Q_i &\equiv A^i(s,t)x^2 + B^i(s,t)xy + \ldots + J^i(s,t)w^2 \\ &\qquad\qquad A^i,\ldots,J^i \in R_{m-1,n-1} \\ Q_i &\equiv (\sum_{j=0}^{m-1}\sum_{k=0}^{n-1} A^i_{j,k}s^jt^k)x^2 + \ldots + (\sum_{j=0}^{m-1}\sum_{k=0}^{n-1} J^i_{j,k}s^jt^k)w^2 \\ Q_i &\equiv \sum_{j=0}^{m-1}\sum_{k=0}^{n-1}(\underbrace{A^i_{j,k}x^2 + \ldots + J^i_{j,k}w^2}_{Q^i_{j,k}(x,y,z,w)})s^jt^k \end{aligned}$$

Selon la méthode décrite à la section précédente on construit une matrice carrée $M(x,y,z,w)$ de taille mn dont les colonnes sont indexées par $1,\ldots,t^m,\ldots,s^{m-1}t^{n-1}$ et dont la i-ème ligne correspond aux mn quadriques $Q^i_{j,k}(x,y,z,w)$ associées à Q_i.

$$M = \begin{array}{c} \\ Q_1 \\ \vdots \\ Q_i \\ \vdots \\ Q_{mn} \end{array} \begin{array}{c} \begin{array}{ccc} & \ldots s^i t^j \ldots & \end{array} \\ \begin{pmatrix} & \vdots & \\ \cdots & Q^i_{j,k}(x,y,z,w) & \cdots \\ & \vdots & \end{pmatrix} \end{array}$$

On a alors le théorème suivant :([CGZ])

Théorème 1 :Supposons : 1)ϕ sans point base
2)ϕ propre (ie génériquement injective)
3)MP de rang maximal
ALORS : i) MQ est aussi de rang maximal
ii) $det(M) = 0$ est l'équation implicite (irréductible) de S

Preuve(constructive) :

• Comme ϕ est propre et sans point base on sait que l'équation implicite irréductible de S est de degré $2mn$ (voir section 2.2).
• D'après le principe de la méthode des surfaces mobiles exposé au 5.1, pour prouver que $det(M) = 0$ est l'équation implicite de S, il suffit de vérifier que $det(M)$ est un polynôme de degré $2mn$. Or comme M est une matrice de taille mn, et que ses coefficients sont des quadriques en x,y,z,w, il suffit simplement de vérifier que $det(M)$ n'est pas nul. Pour ce faire nous aurons d'abord besoin de montrer i).
• Montrons que MQ est de rang maximal.
Notons $[MQ]$ la matrice de l'application MQ

$$MQ : \begin{pmatrix} R^{10}_{m-1,n-1} & \longrightarrow & R_{3m-1,3n-1} \\ (A,B,\ldots,I,J) & \mapsto & (A(s,t)x^2(s,t) + \ldots + J(s,t)w^2(s,t)) \end{pmatrix}$$

dont les lignes sont ordonnées par $s^i t^j i = 0..3m-1, j = 0..3n-1$ et les colonnes par

$$\begin{cases} x^2(s,t)s^i t^j & i = 0 \ldots m-1 \quad j = 0 \ldots n-1 \\ x(s,t)y(s,t)s^i t^j & i = 0 \ldots m-1 \quad j = 0 \ldots n-1 \\ \vdots & \\ z(s,t)w(s,t)s^i t^j & i = 0 \ldots m-1 \quad j = 0 \ldots n-1 \\ w^2(s,t)s^i t^j & i = 0 \ldots m-1 \quad j = 0 \ldots n-1 \end{cases}$$

$$[MQ] = \begin{array}{c} \\ 1 \\ \vdots \\ s^i t^j \\ \vdots \\ s^{3m-1}t^{3n-1} \end{array} \begin{array}{c} \begin{array}{cccccc} x^2(s,t)s^it^j & & x(s,t)y(s,t)s^it^j & & & w^2(s,t)s^it^j \end{array} \\ \left(\begin{array}{c|c|c|c} & & & \\ mn & mn & & mn \\ colonnes & colonnes & \cdots\cdots & colonnes \\ & & & \\ & & & \end{array} \right) \end{array}$$

$[MQ]$ est une matrice $(9mn) \times (10mn)$
Soit $[MQ_w]$ la matrice carrée de taille $9mn$ obtenue à partir de celle de $[MQ]$ en ne retenant que les $9mn$ premières colonnes.
$[MQ_w]$ est la matrice de l'application

$$MQ_w := \left(\begin{array}{ccc} R^9_{m-1,n-1} & \longrightarrow & R_{3m-1,3n-1} \\ (A,B,C,D) & \mapsto & (A(s,t)x^2(s,t) + \ldots + I(s,t)z(s,t)w(s,t)) \end{array} \right)$$

(MQ_w est une restriction de MQ)
On va montrer par l'absurde que $det(MP) \neq 0 \Rightarrow det[MQ_w] \neq 0$ (et donc MQ sera de rang maximal).
Remarque : Par un changement de coordonnées on peut toujours se ramener au cas où le résultant de Dixon de $x(s,t)$,$y(s,t)$,$z(s,t)$, noté $Res_{dix}(x,y,z)$, est non-nul (car on a supposé qu'il n'y avait pas de point base).
Supposons (absurde!) que $det[MQ_w]$.
Alors il existe des polynômes non tous nuls $p_1(s,t), \ldots, p_9(s,t)$ de bidegré (m-1,n-1) tel que :

$$\begin{aligned} p_1x^2 + p_2xy + p_3xz + p_4xw + p_5y^2 + p_6yz + p_7yw + p_8z^2 + p_9zw &= 0 \\ (p_1x + p_2y + p_3z + p_4w)x + (p_5y + p_6z + p_7w)y + (p_8z + p_9w)z &= 0 \end{aligned}$$

Or on a le résultat d'algèbre (admis) suivant ([CGZ]) :

Proposition 7.1 *Soient* $x(s,t) = \sum_{i=0}^m \sum_{j=0}^n a_{i,j}s^it^j$, $y(s,t) = \sum_{i=0}^m \sum_{j=0}^n b_{i,j}s^it^j$, $z(s,t) = \sum_{i=0}^m \sum_{j=0}^n c_{i,j}s^it^j$
trois polynômes de bidegré (m,n) *tels que* $Res_{dix}(x,y,z) \neq 0$.
Supposons de plus qu'il existe trois polynômes A,B,C de bidegré (2m-1,2n-1) tels que

$Ax + By + Cz = 0$.
ALORS il existe h_1,h_2,h_3 *trois polynômes de bidegré (m-1,n-1) tels que*

$$\begin{cases} A &= h_1 z + h_2 y \\ B &= -h_2 x + h_3 z \\ C &= -h_1 x - h_3 y \end{cases}$$

Il existe au moins un des p_i qui n'est pas nul.
Supposons par exemple que $p_9 \neq 0$.
Comme on a vu que l'on pouvait toujours supposer $Res_{dix}(x,y,z) \neq 0$, la proposition admise nous dit qu'il existe h_1,h_2,h_3 de bidegré (m-1,n-1) tels que:

$$h_1 x + h_3 y + p_8 z + p_9 w = 0$$

Donc MP ne serait pas injective, ce qui contredit $det(MP) \neq 0$. Donc $det(MQ_w) \neq 0$.
• Nous pouvons maintenant montrer que $det(M) \neq 0$ et ainsi clôturer la démonstration du théorème 1.
Pour cela nous allons choisir judicieusement les mn quadriques mobiles linéairement indépendantes qui suivent la paramétrisation ϕ, et dont les coefficients constituent la matrice M (car évidemment si pour un choix particulier de mn quadriques mobiles linéairement indépendantes on a $det(M) \neq 0$, alors pour toute façon de choisir les mn quadriques mobiles linéairement indépendantes on aura $det(M) \neq 0$).
Une quadrique mobile de bidegré $(m-1,n-1)$

$$A(s,t)x^2 + \ldots + J(s,t)w^2 = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(A_{i,j}x^2 + \ldots + J_{i,j}w^2)s^i t^j$$

suit la paramétrisation <u>*ssi*</u> $(A,B,C,\ldots,I,J)$ est dans le noyau de MQ

$$\underline{ssi} \qquad [MQ] \begin{pmatrix} A_{0,0} \\ \vdots \\ A_{m-1,n-1} \\ \vdots \\ I_{0,0} \\ \vdots \\ I_{m-1,n-1} \\ J_{0,0} \\ \vdots \\ J_{m-1,n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Or comme les $9mn$ premières colonnes de $[MQ]$ constituent la matrice $[MQ_w]$ qui est inversible, on peut construire des quadriques mobiles qui suivent ϕ en imposant des valeurs à $J_{0,0},\ldots,J_{m-1,n-1}$, et en en déduisant les valeurs que doivent prendre $A_{0,0},\ldots,A_{m-1,n-1},\ldots,I_{0,0},\ldots,I_{m-1,n-1}$.
On définit ainsi $Q_{\alpha,\beta}$ $(\alpha \in \{0..m-1\},\beta \in \{0..n-1\})$ comme étant l'unique quadrique variable de bidegré $(m-1,n-1)$ qui suit la paramétrisation telle que $J_{i,j} = \begin{cases} 0 & si \quad (i,j) \neq (\alpha,\beta), \\ 1 & si \quad (i,j) = (\alpha,\beta). \end{cases}$
Les $Q_{\alpha,\beta}$ sont linéairement indépendantes et de la forme

$$Q_{\alpha,\beta} = w^2 s^\alpha t^\beta + \textit{des termes sans } w^2$$

M est donc de la forme :

$$M = \begin{array}{c} \\ Q_1 \\ \vdots \\ Q_{\alpha,\beta} \\ \vdots \\ Q_{m-1,n-n} \end{array} \begin{pmatrix} w^2+\ldots & & & & \\ & \ddots & & & \\ & & w^2+\ldots & & \\ & & & \ddots & \\ & & & & w^2+\ldots \end{pmatrix}$$

d'où $det(M)$ contient le terme w^{2mn}, et n'est donc pas le polynôme nul.
CQFD

La méthode des quadriques mobiles exprime l'équation implicite sous la forme d'un déterminant de taille mn, ce qui est beaucoup plus rapide à calculer que le déterminant de Dixon, qui permet lui aussi de calculer l'équation implicite, mais qui est de taille $2mn$ (cf section 3.1). C'est ce qui fait l'intérêt de cette méthode.

AMÉLIORATIONS :
Carlos d'Andrea a récemment pu affaiblir les hypothèses du théorème1 ([D]) :
• Si MP est de rang maximal et que ϕ n'est plus génériquement injective mais est génériquement de degré d, alors $det(M) = \lambda F^d$ où $\lambda \in \mathbb{C} - \{0\}$ et $F = 0$ est l'équation implicite irréductible de S.
• Si ϕ est propre alors MP est forcément de rang maximal.

7.3 Cas des paramétrisations de degré total n sans point base

On considère maintenant la paramétrisation d'une surface S de la forme :

$$\phi = \begin{pmatrix} \mathbb{C}^2 & \longrightarrow & \mathbb{P}^3 \\ (s,t) & \mapsto & (x(s,t) : y(s,t) : z(s,t) : w(s,t)) \end{pmatrix}$$

avec $x(s,t)$,$y(s,t)$,$z(s,t)$ et $w(s,t)$ quatre polynômes de degré total n :

$$\begin{array}{ll} x(s,t) = \sum_{0\leq i+j\leq n} a_{i,j} s^i t^j & y(s,t) = \sum_{0\leq i+j\leq n} b_{i,j} s^i t^j \\ z(s,t) = \sum_{0\leq i+j\leq n} c_{i,j} s^i t^j & w(s,t) = \sum_{0\leq i+j\leq n} d_{i,j} s^i t^j \end{array}$$

On suppose ϕ sans point base (même à l'infini).
On appelle " plan mobile de degré p une surface mobile de la forme :

$$A(s,t)x + B(s,t)y + C(s,t)z + D(s,t)w = 0$$

avec A,B,C,D des polynômes de degré total p.
On appelle "quadrique mobile de degré p" une surface mobile de la forme :

$$A(s,t)x^2 + B(s,t)xy + C(s,t)xz + \ldots + I(s,t)zw + J(s,t)w^2 = 0$$

avec A,B,C,$\ldots$,I,J polynômes de degré total p.
Dans toute la suite on ne considérera que des plans mobiles ou des quadriques mobiles de degré $n-1$.
On pose $R_n = \{P \in \mathbb{C}[s,t] / P \text{ de degré } n\}$
On définit :

$$MP = \begin{pmatrix} R_{n-1}^4 & \longrightarrow & R_{2n-1} \\ (A,B,C,D) & \mapsto & (A(s,t)x(s,t) + B(s,t)y(s,t) + C(s,t)z(s,t) + D(s,t)w(s,t)) \end{pmatrix}$$

$$MQ = \begin{pmatrix} R_{n-1}^{10} & \longrightarrow & R_{3n-1} \\ (A,B,C,D) & \mapsto & (A(s,t)x^2(s,t) + B(s,t)x(s,t)y(s,t) + \ldots \\ & & \ldots + I(s,t)z(s,t)w(s,t) + J(s,t)w^2(s,t)) \end{pmatrix}$$

Les plans mobiles de degré $n-1$ qui suivent la paramétrisation sont donnés par le noyau de MP.
Comme $dim(R_{n-1}^4) = 4\binom{n+1}{2} = 2n^2+2n$ et que $dim(R_{2m-1,2n-1}) = \binom{2n+1}{2} = 2n^2+n$, il existe toujours au moins n plans mobiles de degré $n-1$ qui suivent la paramétrisation et qui sont linéairement indépendants, avec égalité si MP est de rang maximal.
Les quadriques mobiles de bidegré $n-1$ qui suivent la paramétrisation sont données

par le noyau de MQ.
Comme $dim(R^{10}_{n-1}) = 10\binom{n+1}{2} = \frac{10n^2+10n}{2}$ et que $dim(R_{3n-1}) = \binom{3n+1}{2} = \frac{9n^2+3n}{2}$, il existe toujours au moins $\frac{n^2+7n}{2}$ quadriques mobiles de degré $n-1$ qui suivent la paramétrisation et qui sont linéairement indépendantes, avec égalité si MQ est de rang maximal.

On cherche à procéder de manière analogue au cas des paramétrisations de bidegré (m,n) pour trouver l'équation implicite de S. Seulement nous allons être obligé d'apporter quelques modifications. En effet cette fois une quadrique mobile Q de degré $n-1$ s'écrit :

$$\begin{aligned} Q &\equiv A(s,t)x^2 + B(s,t)xy + \ldots + J(s,t)w^2 \\ & \qquad\qquad\qquad\qquad\qquad\qquad A,\ldots,J \in R_{n-1} \\ Q &\equiv (\sum_{0\le i+j\le n} A_{j,k}s^jt^k)x^2 + \ldots + (\sum_{0\le i+j\le n} J_{j,k}s^jt^k)w^2 \\ Q &\equiv \sum_{0\le i+j\le n} (\underbrace{A_{j,k}x^2 + \ldots + J_{j,k}w^2}_{Q_{j,k}(x,y,z,w)})s^jt^k \end{aligned}$$

de même un plan mobile L de degré $n-1$ s'écrit :

$$\begin{aligned} L &\equiv A(s,t)x + B(s,t)y + C(s,t)z + D(s,t)w \\ & \qquad\qquad\qquad\qquad\qquad\qquad A,B,C,D \in R_{n-1} \\ L &\equiv (\sum_{0\le i+j\le n} A_{j,k}s^jt^k)x + \ldots + (\sum_{0\le i+j\le n} D_{j,k}s^jt^k)w \\ L &\equiv \sum_{0\le i+j\le n} (\underbrace{A_{j,k}x + B_{j,k}x + C_{j,k}x + D_{j,k}w}_{L_{j,k}(x,y,z,w)})s^jt^k \end{aligned}$$

Une quadrique mobile est donnée par $\frac{(n+1)n}{2}$ coefficients (les $Q_{j,k}$). Si on voulait procéder comme précédemment il faudrait donc construire une matrice carrée de taille $\frac{(n+1)n}{2}$ avec les coefficients de $\frac{(n+1)n}{2}$ quadriques mobiles suivant la paramétrisation, puis calculer son déterminant. Or on obtiendrait ainsi un polynôme de taille $(n+1)n$, alors que l'équation implicite irréductible de S est de degré n^2 (si ϕ est propre). Il faut donc réduire le degré du déterminant de n. Pour cela on va remplacer n quadriques mobiles par n plans mobiles, puisque l'on sait qu'un tel nombre de plans mobiles

linéairement indépendants suivant la paramétrisation existent toujours.
Pour le choix des $\frac{(n+1)n}{2} - n = \frac{(n-1)n}{2}$ quadriques mobiles on a a priori le choix, puisque $dim(ker(MQ)) \geq \frac{n^2+7n}{2}$. Mais observons que si on choisit une quadrique mobile qui soit de type

$$xp(x,y,z,w,s,t), yp(x,y,z,w,s,t), zp(x,y,z,w,s,t), \quad ou \quad wp(x,y,z,w,s,t),$$

avec $p(x,y,z,w,s,t)$ un plan mobile dans l'espace V engendré par les n plans mobile qui ont servi à construire M, alors $det(M) = 0$.
Donc il faut choisir nos $\frac{(n-1)n}{2}$ quadriques mobiles dans $ker(MQ)\backslash V$, avec $dim(ker(MQ)\backslash V) \geq \frac{(n+7)n}{2} - 4n = \frac{(n-1)n}{2}$ (avec égalité si MQ est de rang maximal).

Soit L_i, $i = 1 \ldots n$ des plans mobiles et Q_i, $i = 1 \ldots \frac{n(n-1)}{2}$ des quadriques mobiles choisies comme expliqué précédemment :
On note

$$L_i \equiv \sum_{0 \leq i+j \leq n} \underbrace{(A^i_{j,k}x + B^i_{j,k}y + C^i_{j,k}z + D^i_{j,k}w)}_{L^i_{j,k}(x,y,z,w)} s^j t^k \quad i = 1 \ldots n$$

$$Q_i \equiv \sum_{0 \leq i+j \leq n} \underbrace{(A^i_{j,k}x^2 + \ldots + J^i_{j,k}w^2)}_{Q^i_{j,k}(x,y,z,w)} s^j t^k \qquad i = 0 \ldots \frac{(n+1)}{2}$$

$$M = \begin{array}{c} \\ Q_1 \\ \vdots \\ \vdots \\ Q_i \\ \vdots \\ Q_{\frac{(n-1)n}{2}} \\ \\ L_1 \\ \vdots \\ L_i \\ \vdots \\ L_n \end{array} \begin{array}{c} s^i t^j \\ \left(\begin{array}{ccc} & \vdots & \\ & \vdots & \\ \cdots\cdots & Q^i_{j,k}(x,y,z,w) & \cdots\cdots \\ & \vdots & \\ \hline & & \\ & \vdots & \\ \cdots\cdots & L^i_{j,k}(x,y,z,w) & \cdots\cdots \\ & \vdots & \\ & & \end{array} \right) \end{array}$$

On a alors le théorème pendant de celui de la section 7.2 :

Théorème 2 :Supposons : 1)ϕ sans point base
2)ϕ propre (ie génériquement injective)
3)MP de rang maximal
ALORS : i) MQ est aussi de rang maximal
ii) si M est construite comme expliquée ci-dessus alors
$det(M) = 0$ est l'équation implicite (irréductible) de S.

La démonstration de ce théorème va nécessiter l'utilisation de la proposition admise suivante , proposition pendante de celle de la section 7.2 ([CGZ]) :

Proposition 7.2 *Soit x,y,z trois polynômes ce $\mathbb{C}[s,t]$ de degré total n.*
Supposons que leur résultant (de Macaulay) soit non nul.
Soit A,B,$C \in \mathbb{C}[s,t]$ tels que $Ax + By + Cz = 0$.
ALORS il existe h_1,h_2,h_3 trois polynômes de $\mathbb{C}[s,t]$ tels que

$$\begin{cases} A &= h_1 z + h_2 y, \\ B &= -h_2 x + h_3 z, \\ C &= -h_1 x - h_3 y. \end{cases}$$

De plus si A,B,C sont de degré inférieur à k on peut choisir h_1,h_2,h_3 de degré inférieur à $k - n$.

Preuve(constructive) :

• Comme ϕ est propre et sans point base on sait que l'équation implicite irréductible de S est de degré n^2 (voir section 2-2).
• D'après le principe de la méthode des surfaces mobiles exposé au 5-1, pour prouver que $det(M) = 0$ est l'équation implicite de S il suffit de vérifier que $det(M)$ est un polynôme de degré n^2.
Or on a construit M de telle façon que si $det(M)$ est non nul alors $det(M)$ est de degré n^2. Il suffit donc de vérifier que $det(M) \neq 0$.
Pour le voir nous allons choisir "judicieusement" les L_i $(i = 1..n)$ et les les Q_i $(i = 1..\frac{(n-1)n}{2})$, comme pour la démonstration du théorème1.

Commençons par introduire quelques notations :
On note $[MP]$ la matrice de l'application MP

$$MP = \begin{pmatrix} R_{n-1}^4 & \longrightarrow & R_{2n-1} \\ (A,B,C,D) & \mapsto & (A(s,t)x(s,t) + \ldots + D(s,t)w(s,t)) \end{pmatrix}$$

dont les lignes sont ordonnées par les $s^k t^l (0 \leq k+l \leq 2n-1)$ et les colonnes par

$$\begin{cases} x(s,t)s^i t^j & 0 \leq i+j \leq n-1 \\ \vdots & \\ w(s,t)s^i t^j & 0 \leq i+j \leq n-1 \end{cases}$$

$$[MP] = \begin{array}{c} \\ \vdots \\ s^k t^l \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccc} x(s,t)s^i t^j & y(s,t)s^i t^j & z(s,t)s^i t^j & w(s,t)s^i t^j \end{array} \\ \left(\begin{array}{c|c|c|c} \frac{(n+1)n}{2} & \frac{(n+1)n}{2} & \frac{(n+1)n}{2} & \frac{(n+1)n}{2} \\ colonnes & colonnes & colonnes & colonnes \\ & & & \end{array} \right) \end{array}$$

On pose $[MQ]$ la matrice de l'application MQ

$$MQ = \begin{pmatrix} R_{n-1}^{10} & \longrightarrow & R_{3n-1} \\ (A,B,\ldots,I,J) & \mapsto & (A(s,t)x^2(s,t) + \ldots + J(s,t)w^2(s,t)) \end{pmatrix}$$

dont les lignes sont ordonnées par $s^k t^l (0 \leq k+l \leq 2n-1)$ et les colonnes par

$$\begin{cases} x^2(s,t)s^i t^j & 0 \leq i+j \leq 3n-1 \\ x(s,t)y(s,t)s^i t^j & 0 \leq i+j \leq 3n-1 \\ \vdots & \\ z(s,t)w(s,t)s^i t^j & 0 \leq i+j \leq 3n-1 \\ w^2(s,t)s^i t^j & 0 \leq i+j \leq 3n-1 \end{cases}$$

$$[MQ] = \begin{array}{c} \\ \vdots \\ s^k t^l \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} x^2(s,t)s^i t^j & x(s,t)y(s,t)s^i t^j & & & w^2(s,t)s^i t^j \end{array} \\ \left(\begin{array}{c|c|c|c|c} \frac{(n+1)n}{2} & \frac{(n+1)n}{2} & & & \frac{(n+1)n}{2} \\ colonnes & colonnes & \cdots\cdots & & colonnes \\ & & & & \end{array} \right) \end{array}$$

Comme dans la preuve du théorème 1 de la section 7.2, puisque ϕ est sans point base on peut se ramener au cas où le résultant (de Macaulay) de $x(s,t)$,$y(s,t)$,$z(s,t)$ est

non nul.
On a alors :
Lemme 1 : *les* $\frac{3n(n+1)}{2}$ *première colonnes de* $[MP]$ *correspondant à* $x(s,t)s^it^j$,$y(s,t)s^it^j$,$z(s,t)s^it^j \quad 0 \leq i+j \leq n-1$ *sont linéairement indépendantes.*
Preuve :

Si les $\frac{3n(n+1)}{2}$ première colonnes de $[MP]$ n'étaient pas indépendantes il existerait des polynômes $p_1(s,t)$,$p_2(s,t)$,$p_3(s,t)$ de degré $n-1$ (ou moins),non tous nuls, tels que :

$$p_1(s,t)x(s,t) + p_2(s,t)y(s,t) + p_3(s,t)z(s,t) = 0$$

Comme on peut se ramener au cas où le résultant de x(s,t),y(s,t),z(s,t) est non nul, l'application de la proposition 2 nous dit qu'il existe 3 polynômes h_1,h_2,h_3 de degré inférieur ou égal à -1 ,donc nuls, tels que :

$$\begin{cases} p_1 &= \quad h_1 z + h_2 y \\ p_2 &= -h_2 x + h_3 z \\ p_3 &= -h_1 x - h_3 y \end{cases}$$

Donc $p_1(s,t) = p_2(s,t) = p_3(s,t) \equiv 0$, contradiction!

Soit $I \subset \{(k,l)/0 \leq k+l \leq n-1\}$ un ensemble d'indices avec $card(I) = n$.
On définit $[MP]_I$ comme étant la sous-matrice carrée extraite de $[MP]$ en supprimant les colonnes correspondant aux $w(s,t)s^it^j, \quad (i,j) \in I$.
On définit $[MQ]_I$ comme étant la sous-matrice carrée extraite de $[MQ]$ en supprimant les colonnes correspondant aux

$$\begin{cases} x(s,t)w(s,t)s^it^j & ,(i,j) \in I \\ y(s,t)w(s,t)s^it^j & ,(i,j) \in I \\ \qquad \vdots & \\ z(s,t)w(s,t)s^it^j & ,(i,j) \in I \end{cases}$$

$$\{ \; w(s,t)^2 s^i t^j \quad ,0 \leq i+j \leq n-1$$

Comme par hypothèse MP est de rang maximal,du lemme1 on déduit qu'il existe un ensemble $I \subset \{(k,l)/0 \leq k+l \leq n-1\}$ tel que $[MP]_I$ soit une matrice inversible. I désignera désormais cet ensemble.
Lemme 2 : $[MQ]_I$ *est inversible.*
Preuve :

Par l'absurde :
Supposons que $[MQ]_I$ ne soit pas inversible.
Alors il existe des polynômes $p_1(s,t),\ldots,p_9(s,t)$ de degré $n-1$ (ou moins),non tous nuls, tels que :

$$\begin{aligned} p_1x^2+p_2xy+p_3xz+p_4xw+p_5y^2+p_6yz+p_7yw+p_8z^2+p_9zw &= 0 \\ (p_1x+p_2y+p_3z+p_4w)x+(p_5y+p_6z+p_7w)y+(p_8z+p_9w)z &= 0 \end{aligned}$$

De plus les monômes dont les exposants sont dans I n'interviennent pas dans $p_7(s,t)$,$p_8(s,t)$,$p_9(s,t)$.
Au moins un des p_i n'est pas nul. Supposons que ce soit p_9 (les autres cas se traitent de la même manière) :
Comme on peut s'est ramené au cas où le résultant de x(s,t),y(s,t),z(s,t) est non nul, l'application de la proposition 2 nous dit qu'il existe des polynômes h_1,h_3 de degré inférieur ou égal à n-1 , tels que : $h_1x+h_3y+p_8z+p_9w=0$.
Comme les monômes dont les exposants sont dans I n'interviennent pas dans $p_9(s,t)$, on déduirait de l'équalité précédentes que $[MP]_I$ n'est pas injective, contradiction!
Donc $[MQ]_I$ est inversible.

D'après le lemme2 on a bien MQ de rang maximal.
Il reste à montrer ii).
Soit

$$Q(x,y,z,w,s,t)=(\sum_{0\le i+j\le n}A_{j,k}s^jt^k)x^2+\ldots+(\sum_{0\le i+j\le n}J_{j,k}s^jt^k)w^2$$

une quadrique mobile de degré $n-1$. Q suit la paramétrisation

$$Q \text{ suit la paramétrisation } \underline{ssi} \quad [MQ]\begin{pmatrix} A_{0,0} \\ \vdots \\ A_{m-1,n-1} \\ \vdots \\ I_{0,0} \\ \vdots \\ I_{m-1,n-1} \\ J_{0,0} \\ \vdots \\ J_{m-1,n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Comme $[MQ]_I$ est inversible, on peut imposer des valeurs aux coefficients

$$\begin{cases} G_{i,j}, H_{i,j}, I_{i,j} & (i,j) \in I \\ J_{i,j} & 0 \leq i+j \leq n-1 \end{cases}$$

et résoudre un système pour déterminer les valeurs que doivent prendre les autres coefficients pour que la quadrique mobile suive la paramétrisation.
Soit (i_0,j_0) tel que $0 \leq i_0 + j_0 \leq n-1$, mais avec $(i_0,j_0) \notin I$.
Imposons les valeurs

$$\begin{cases} G_{i,j} = H_{i,j} = I_{i,j} = 0 & \text{pour} (i,j) \in I \\ J_{i,j} = 0 & \text{pour tout } 0 \leq i+j \leq n-1, \text{ sauf pour} (i_0,j_0) \\ J_{i_0,j_0} = 1 & \end{cases}$$

On construit ainsi $\frac{(n-1)n}{2}$ quadriques mobiles Q_{i_0,j_0} linéairement indépendantes, de la forme :

$$Q_{i_0,j_0} = w^2 s^{i_0} t^{j_0} + \text{ des termes ne contenant pas } w^2.$$

De manière analogue, comme $[MP]_I$, on peut construire n plans mobiles de type :

$$L_{i,j} = w s^i t^j + \text{ des termes ne contenant pas } w s^k t^l \text{ avec } (k,l) \in I.$$

Ainsi la matrice M associée à ces plans mobiles et ces quadriques mobiles est de la forme

$$M = \begin{array}{c} \\ \vdots \\ Q_{i,j} \\ \vdots \\ \\ L_1 \\ \vdots \\ L_n \end{array} \begin{pmatrix} w^2 + \dots & & & & \\ & \ddots & & & \\ & & w^2 + \dots & & \\ \hline & & & w + \dots & \\ & & & & \ddots \\ & & & & & w^2 + \dots \end{pmatrix}$$

Le déterminant de cette matrice contient le terme w^{n^2}, donc n'est pas nul.
CQFD

AMÉLIORATIONS :

Carlos d'Andrea a pu montrer les mêmes améliorations sur les hypothèses du théorème 2 que celles sur les hypothèses du théorème 1 ([D]) :
• Si MP est de rang maximal et que ϕ n'est plus génériquement injective mais est génériquement de degré d, alors $det(M) = \lambda F^d$ où $\lambda \in \mathbb{C} - \{0\}$ et $F = 0$ est l'équation implicite irréductible de S.
• Si ϕ est propre alors MP est forcément de rang maximal.

8 Bezoutiens et équations implicites

Nous allons maintenant présenter une méthode permettant de trouver un multiple de l'équation implicite associée à une surface paramétrée. Cette méthode repose sur l'utilisation de matrices bezoutiennes.

Soit $R := \mathbb{C}[t_1,\ldots,t_{n-1}] = \mathbb{C}[\mathbf{t}]$ l'anneau des polynômes sur $\mathbb{C}$ en les variables $t_1,\ldots,t_{n-1}$. Par l'introduction de nouvelles variables $z = (z_1,\ldots,z_{n-1})$ nous identifierons l'algèbre $R \otimes_{\mathbb{C}} R$ avec $\mathbb{C}[t,z] = [t_1,\ldots,t_{n-1},z_1,\ldots,z_{n-1}]$.

Définition 8.1 *Soit $h_1,\ldots,h_n$ des polynômes de $R := \mathbb{C}[t_1,\ldots,t_{n-1}]$. On appelle bezoutien de $h_1,\ldots,h_n$ le polynôme de $R \otimes_{\mathbb{C}} R$ noté $\Theta_{h_1,\ldots,h_n}$ définit par :*

$$\Theta_{h_1,\ldots,h_n}(t,z) = \begin{vmatrix} h_1(t) & \theta_1(h_1)(t,z) & \ldots & \theta_{n-1}(h_1)(t,z) \\ \vdots & \vdots & \vdots & \vdots \\ h_n(t) & \theta_1(f_n)(t,z) & \ldots & \theta_{n-1}(h_n)(t,z) \end{vmatrix}$$

où

$$\theta_i(h_j)(t,z) := \frac{h_j(z_1,\ldots,z_{i-1},t_i,\ldots,t_{n-1}) - h_j(z_1,\ldots,z_i,t_{i+1},\ldots,t_{n-1})}{t_i - z_i}.$$

La matrice bezoutienne de $h_1,\ldots,h_n$ est la matrice $B_{h_1,\ldots,h_n} = (\theta_{\alpha,\beta})_{\alpha,\beta}$, où les $\theta_{\alpha,\beta}$ sont les éléments de $\mathbb{C}$ définis par $\Theta_{h_1,\ldots,h_n}(t,z) = \sum \theta_{\alpha,\beta} t^\alpha z^\beta$.
Lorsque les $h_2,\ldots,h_n$ seront fixés on notera aussi $\Theta_{h_1,\ldots,h_n} = \Theta_{h_1}$ et $B_{h_1,\ldots,h_n} = B_{h_1}$.

Définition 8.2 *Soit $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ et $\mathbf{w} = (w_j)_{j\in\mathbb{N}}$ deux $\mathbb{C}$-bases de R, et soit*

$$\Theta_{h_1,\ldots,h_n} = \sum_{i,j} \nu_{ij} v_i \otimes w_j, \quad \nu_{ij} \in \mathbb{C}$$

la décomposition du bezoutien dans ces bases. La matrice des coefficients $(\nu_{ij})_{i,j}$ sera notée $B^{\mathbf{v},\mathbf{w}}_{h_1,\ldots,h_n}$.

Nous aurons bientôt besoin du lemme suivant, dont on peut trouver la démonstration par exemple dans [BEM] :

lemme *Soit $I = (f_1,\ldots,f_{n-1})$ un idéal de R tel que le $\mathbb{C}$-espace vectoriel $A = R/I$ soit de dimension finie D. Alors il existe deux bases $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ et $\mathbf{w} = (w_j)_{j\in\mathbb{N}}$ de R telles que $(\overline{v_1},\ldots,\overline{v_D}),(\overline{w_1},\ldots,\overline{w_D})$ soient des bases de A, $v_i,w_i \in I$ pour $i > D$, et telles que pour tout f_0 dans R on ait la matrice $B^{\mathbf{v},\mathbf{w}}_{h_1,\ldots,h_n}$ qui soit de la forme*

$$M = \begin{array}{c} \\ w_1 \\ \vdots \\ w_D \\ \\ w_{D+1} \\ \vdots \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} v_1,\ldots,v_D & \quad v_{D+1}\cdots \end{array} \\ \left(\begin{array}{c|c} & \\ M_{f_0} & \mathbf{0} \\ & \\ \hline & \\ \mathbf{0} & L_{f_0} \\ & \end{array}\right) \end{array}$$

où M_{f_0} est la matrice de multiplication par f_0 dans la base $(\overline{v_1},\ldots,\overline{v_D})$ de A.

A partir de maintenant on sera toujours dans le cas $n = 3$.
Donnons-nous la paramétrisation d'une surface

$$\left\{\begin{array}{lcl} x_1 & = & f_1(\mathbf{t})/f_0(\mathbf{t}) \\ x_2 & = & f_2(\mathbf{t})/f_0(\mathbf{t}) \\ x_3 & = & f_3(\mathbf{t})/f_0(\mathbf{t}) \end{array}\right.$$

avec $f_0,\ldots,f_4 \in \mathbb{C}[\mathbf{t}] = \mathbb{C}[t_1,t_2]$ et $PGCD(f_1,\ldots,f_4) = 1$.
Posons comme d'habitude

$$h_i(\mathbf{t}) = f_0(\mathbf{t})x_i - f_i(\mathbf{t}), \quad i = 1,2,3.$$

On a alors le théorème suivant :

Théorème 8.1 *Supposons que $PGCD(f_0,f_2,f_3) = 1$. Alors tout mineur maximal non-nul de la matrice bezoutienne B_{h_1,h_2,h_3} est un multiple de l'équation implicite.*

Remarque : le théorème reste vrai même si $PGCD(f_0,f_2,f_3) \neq 1$, mais l'auteur de ce mémoire ne sait pas le démontrer. Ceci étant dit il est toujours possible de se ramener à cette hypothèse en posant $f_3' = f_3 + cf_1$ et en choisissant correctement c (car $PGCD(f_0,f_1,f_2,f_3) = 1$).

Preuve du théorème :

• On désigne par r la taille d'un mineur maximal non-nul de la matrice bezoutienne B_{h_1,h_2,h_3}
• Comme $PGCD(f_0,f_2,f_3) = 1$, pour x_2,x_3 génériques on a $PGCD(f_0x_2 - f_2, f_0x_3 -$

$f_3) = 1$. On en déduit par le théorème de Bezout que pour des valeurs génériques de x_2,x_3 on a $\mathbb{C}[\mathbf{t}]/(h_2,h_3)$ qui est de dimension finie.

• Fixons pour toute la suite x_2,$x_3 \in \mathbb{C}$ génériques. On peut donc appliquer le lemme : il existe deux bases $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ et $\mathbf{w} = (w_j)_{j\in\mathbb{N}}$ de R telles que la matrice $B^{\mathbf{v},\mathbf{w}}_{h_1,h_2,h_3}$ qui soit de la forme

$$M = \begin{array}{c} \\ w_1 \\ \vdots \\ w_D \\ \\ w_{D+1} \\ \vdots \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} v_1,\ldots,v_D & v_{D+1}\cdots \end{array} \\ \left(\begin{array}{c|c} & \\ M_{h_1} & \mathbf{0} \\ & \\ \hline & \\ \mathbf{0} & L_{h_1} \\ & \end{array}\right) \end{array}.$$

Cette décomposition est valable pour tout $x_1 \in \mathbb{C}$.
(par contre les bases $\mathbf{v}$ et $\mathbf{w}$ dépendent des valeurs de x_2 et de x_3).

• Soit r_1 (respectivement r_2) le rang de M_{h_1} (respectivement le rang de L_{h_1}) pour x_1 générique. On a :

$$r = r_1 + r_2$$

On sait que les valeurs propres de la matrice M_{h_1} sont les $h_1(\zeta_i)$, où les ζ_i,$i = 1\ldots,D$ sont les solutions communes de $h_2 = h_3 = 0$.
Si la paramétrisation admet m points bases, comme ces m points bases sont toujours des solutions de $h_2 = h_3 = 0$, ils font partie de $\{\zeta_i / i = 1\ldots,D\}$, et ce pour tout x_1. Comme un point base vérifie aussi $h_1 = 0$, les points bases correspondent à des valeurs propres nulles de M_{h_1}.
Comme pour un choix générique de x_1, h_1 n'a pas de zéro commun avec h_2,h_3 autre que les points bases, la matrice M_{h_1} est de rang générique $D - m$.
Par conséquent

$$r_1 = D - m \qquad r_2 = r - D + m.$$

• Supposons que x_1 corresponde à une valeur telle que h_1,h_2,h_3 aient une solution commune autre que les points bases (c'est notamment le cas si le point (x_1,x_2,x_3) est dans l'image de la paramétrisation) : alors le rang de M_{h_1} est strictement inférieur à $D - m$, et comme le rang de L_{h_1} ne peut excéder sa valeur générique, on en déduit que pour cette spécialisation de x_1,x_2,x_3 tous les mineurs de taille r de la matrice $B^{\mathbf{v},\mathbf{w}}_{h_1,h_2,h_3}$ sont nuls.
Ceci montre que tous les mineurs de taille r de la matrice $B^{\mathbf{v},\mathbf{w}}_{h_1,h_2,h_3}$ sont des multiples

de l'équation implicite de la surface.
CQFD.

Une fois que l'on connaît un multiple de l'équation implicite il reste à factoriser celui-ci et à déterminer le facteur correspondant à l'équation de la surface (à propos de ce dernier point, revoir ce qui a été dit au paragraphe 4.2).

9 Implicitisation par le résultant résiduel

Nous allons présenter une méthode de calcul de l'équation implicite d'une surface définie par une paramétrisation qui est efficace dans le cas avec points bases sous certaines hypothèses. Pour cela nous aurons besoin de la notion de résultant résiduel.

9.1 Résultant résiduel (sur $\mathbb{P}^2$)

Soit $R = \mathbb{C}[x_0,x_1,x_2]$ un anneau polynomial, et soit $G = (g_1,\ldots,g_n)$ l'idéal homogène de R engendré par les g_i avec $deg(g_i) = k_i$ et $k_1 \geq \ldots \geq k_n$. On note $x = (x_0,x_1,x_2)$ et $|\alpha| = \alpha_1 + \alpha_2 + \alpha_3$ pour $\alpha = (\alpha_1,\alpha_2,\alpha_3) \in \mathbb{N}^3$.
Soit f_1,f_2,f_3 trois polynômes génériques de l'idéal $G = (g_1,\ldots,g_n)$, de degré respectivement d_1,d_2,d_3. Par "polynôme générique de $G = (g_1,\ldots,g_n)$" on veut dire que f_j s'écrit sous la forme $f_j(s,t,u) = \sum_{i=1}^{n} h_{i,j}(s,t,u)g_i(s,t,u)$ avec $h_{i,j} = \sum_{|\alpha|=d_j-k_i} c_\alpha^{i,j} x^\alpha$ polynôme générique homogène de degré $d_j - k_i$.
Dans toute la suite $G = (g_1,\ldots,g_n)$ sera supposé être saturé et être localement intersection complète (*ie* localement le nombre de générateurs de G est égal à sa codimension).

Théorème-définition: *Il existe un polynôme irréductible en les variables $c_\alpha^{i,j}$, noté $\widetilde{Res}(f_1,f_2,f_3)$ tel que*
$\widetilde{Res}(f_1,f_2,f_3) = 0 \Longleftrightarrow (f_1,f_2,f_3)^{sat} \neq (g_1,\ldots,g_n)^{sat}$.
$\Longleftrightarrow$ *les f_i s'annulent en un point de $\mathbb{P}^n$ qui n'est pas dans $V(G)$ (les points sont comptés avec multiplicité).*

Le résultant résiduel nous permet donc de déterminer si les f_j ont un zéro commun qui ne soit pas trivial, c'est-à-dire qui ne soit pas un zéro commun des g_i.
Nous allons maintenant expliquer comment construire ce résultant résiduel.
Rappelons d'abord que dans le cas du résultant "classique" sur $\mathbb{P}^2$ on a une résolution de $F = (f_1,f_2,f_3)$ du type:

$$\begin{array}{ccccccccccc} 0 & \rightarrow & R & \stackrel{\phi}{\rightarrow} & R^3 & \stackrel{\psi}{\rightarrow} & R^3 & \stackrel{(f_1,f_2,f_3)}{\longrightarrow} & F & \rightarrow & 0 \\ & & & & & & (a,b,c) & \stackrel{\varphi}{\mapsto} & af_1+bf_2+cf_3 & & \end{array}$$

où, avec des notations classiques:

$$\phi : \begin{pmatrix} R(e_1\wedge e_2\wedge e_3) & \longrightarrow & R(e_2\wedge e_3)\oplus R(e_1\wedge e_3)\oplus R(e_1\wedge e_2) \\ e_1\wedge e_2\wedge e_3 & \mapsto & f_1(e_2\wedge e_3) - f_2(e_1\wedge e_3) + f_3(e_1\wedge e_2) \end{pmatrix}$$

$$\psi : \begin{pmatrix} R(e_2 \wedge e_3) \oplus R(e_1 \wedge e_3) \oplus R(e_1 \wedge e_2) & \longrightarrow & R(e_1 \wedge e_2 \wedge e_3) \\ e_i \wedge e_j & \mapsto & f_i e_j - f_j e_i \end{pmatrix}.$$

La dernière application de cette résolution nous permet de construire le résultant de (f_1,f_2,f_3) : en notant $R^{(n)}$ l'ensemble des polynômes homogènes de degré n, φ induit par restriction une application

$$\begin{pmatrix} R^{(d_2+d_3-2)} \oplus R^{(d_1+d_3-2)} \oplus R^{(d_1+d_2-2)} & \rightarrow & R^{(d_1+d_2+d_3-2)} \\ (a,b,c) & \overset{\varphi}{\mapsto} & af_1 + bf_2 + cf_3 \end{pmatrix}.$$

Appelons M la matrice de cette application dans les bases canoniques

$$M = \begin{pmatrix} | & | & | \\ f_1 & f_2 & f_3 \\ | & | & | \end{pmatrix}.$$

On a $Resultant(f_1,f_2,f_3) = PGCD$(mineurs maximaux de M).

Pour construire le résultant résiduel on va procéder de manière analogue, mais au lieu de construire une résolution de F on construit une résolution de $(F : G)$ (le cas classique correspondant en fait à $G = R$ car $(F : R) = F$). Les démonstrations des résultats présentés se trouvent dans [Buse] :
La construction qui suit n'est valable que lorsque G est arithmétiquement Cohen-Macaulay de codimension 2, *ie* lorsque G est complètement déterminé par ses premières syzygies.

étape 1 : comme on a supposé que G est arithmétiquement Cohen-Macaulay de codimension 2 on a une résolution de type :

$$0 \rightarrow \bigoplus_{i=1}^{n-1} R(-l_i) \overset{\phi}{\rightarrow} \bigoplus_{i=1}^{n} R(-k_i) \overset{(g_1,\ldots,g_n)}{\rightarrow} G \rightarrow 0$$

On construit la matrice à n lignes et $n-1$ colonnes de l'application ϕ dans les bases canoniques. On note

$$M_1 = (k_{i,j}(x_0,x_1,x_2))_{i=1\ldots n, j=1\ldots n-1}.$$

étape 2 : D'après la définition des $h_{i,j}$ on peut écrire

$$[f_1,f_2,f_3] = [g_1,\ldots,g_n] \cdot M_2$$

où M_2 désigne la matrice de taille (n,3) :

$$M_2 = (h_{i,j}(x_0,x_1,x_2))_{i=1\ldots n, j=1\ldots 3}.$$

Les $h_{i,j}$ correspondent aux coefficients de la division de f_j par l'idéal $(g_1,\ldots,g_n)$.
Soit ψ l'application déduite de la matrice $M_2 : \bigoplus_{i=1}^{3} R(-d_i) \stackrel{M_2}{\to} \bigoplus_{i=1}^{n} R(-k_i)$.
On peut alors montrer que l'on a la présentation suivante de F/G :

$$\bigoplus_{i=1}^{3} R(-d_i) \bigoplus_{i=1}^{n-1} R(-l_i) \stackrel{\psi\oplus\phi}{\longrightarrow} \bigoplus_{i=1}^{n} R(-k_i) \stackrel{(g_1,\ldots,g_n)}{\longrightarrow} F/G \to 0$$

La matrice associée à $\psi \oplus \phi$ est $M := M_1||M_2$, où .||. représente la concaténation de deux matrices.
De cette présentation on déduit une résolution libre graduée de $(F : G)$ dont la dernière application est :

$$\begin{array}{ccccccc} \ldots & \longrightarrow & \bigoplus_{i_1<\ldots<in} Re_{i_1} \wedge \ldots \wedge e_{i_n} & \stackrel{\eta}{\longrightarrow} & (F:G) & \longrightarrow & 0 \\ & & e_{i_1} \wedge \ldots \wedge e_{i_n} & \stackrel{\eta}{\mapsto} & \Delta_{i_1,\ldots,i_n} & & \end{array}$$

où $\Delta_{i_1,\ldots,i_n}$ représente le mineur de M obtenu en ne gardant que les colonnes $i_1,\ldots,i_n$.

étape 3 : soit $\nu = d_1 + d_2 + d_3 - 2(k_n + 1)$.
Alors l'application η en degré ν est donnée dans les bases monomiales par la matrice

$$M_\nu = \left(\begin{array}{c|c|c|c} & & & \\ \cdot\Delta_{1,\ldots,n} & \ldots & \cdot\Delta_{i_1,\ldots,i_n} & \ldots \\ & & & \end{array} \right).$$

où le bloc de colonnes associé à "$\cdot\Delta_{i_1,\ldots,i_n}$" correspond à la multiplication par $\Delta_{i_1,\ldots,i_n}$.

Proposition 9.1 *$\widetilde{Res}(f_1,f_2,f_3)$=PGCD(mineurs maximaux de M_ν).*

9.2 Application à l'implicitisation

Soit S une surface paramétrée par

$$x = \frac{p_1(x_0,x_1,x_2)}{p_4(x_0,x_1,x_2)} \quad y = \frac{p_2(x_0,x_1,x_2)}{p_4(x_0,x_1,x_2)} \quad x = \frac{p_3(x_0,x_1,x_2)}{p_4(x_0,x_1,x_2)}$$

où p_1,p_2,p_3,p_4 sont quatre polynômes homogènes de $\mathbb{C}[x_0,x_1,x_2]$ de même degré d. Soit F(x,y,z) l'équation implicite irréductible de S. On pose comme d'habitude

$$H_1 := p_4(x_0,x_1,x_2)x - p_1(x_0,x_1,x_2) \tag{16}$$
$$H_2 := p_4(x_0,x_1,x_2)y - p_2(x_0,x_1,x_2) \tag{17}$$
$$H_3 := p_4(x_0,x_1,x_2)z - p_3(x_0,x_1,x_2). \tag{18}$$

Ce qui faisait échouer la méthode utilisant le résultant de Macaulay en présence de points bases, c'est que les points bases étaient toujours des zéros des H_i, et ce quelles que soient les valeurs données à x,y et z. Le résultant résiduel va justement nous permettre de savoir quand le système constitué des H_i admet une solution non-triviale, i.e. une solution qui ne soit pas un point base.
Soit $G := (p_1,p_2,p_3,p_4)^{sat}$.
Soit $g_1,\ldots,g_n \in \mathbb{C}[x_0,x_1,x_2]$ tels que $G = (g_1,\ldots,g_n)$ avec n minimal et degré$(g_i) = k_i$.

Proposition 9.2 *Supposons que G soit une intersection complète locale avec $d \geq k_1 \geq \ldots \geq k_n$ et $d \geq k_n + 1$. Alors il existe $\beta \in \mathbb{N}^*$ tel que :*

$$\widetilde{Res}(H_1,H_2,H_3) = F^\beta$$

Si la paramétrisation est propre, on a $\beta = 1$.

On obtient donc une nouvelle méthode d'implicitisation qui a l'avantage de marcher en présence de points bases (sous certaines hypothèses). Théoriquement elle fournit exactement l'équation implicite comme PGCD des mineurs maximaux de la matrice M_ν associée à la paramétrisation, cependant en pratique calculer TOUS les mineurs maximaux (et il peut y en avoir énormément) pour ensuite calculer leur PGCD est beaucoup trop coûteux, et on se retrouve facilement "out of memory". C'est pourquoi nous préconisons plutôt de calculer un seul des mineurs maximaux, puis de le factoriser (le gain de temps est considérable : voir à ce sujet le commentaire de l'exemple 5 du chapitre 10). C'est cette méthode qui sera appliquée dans les exemples du prochain chapitre.

10 Comparaison numérique des méthodes étudiées et conclusion

10.1 Résultats numériques

Les exemples qui suivent ont été traités sur deux machines différentes : la première est un Pentium III (1 GHz) avec 512Mo de sdram, la seconde est un Pentium IV (GHz) avec 256Mo de sdram. Évidemment, pour un exemple de paramétrisation de surface donné, toutes les méthodes ont été testées sur la même machine, pour que la comparaison est un sens (et à chaque fois nous préciseront laquelle des deux machines a été utilisée).
Par contre toutes les méthodes n'ont pas été programmées à l'aide du même logiciel : MAPLE, Macaulay2 et Magma ont été utilisés. On peut critiquer cet aspect et estimer que pour que la comparaison soit valable il aurait fallu programmer toutes les méthodes soit en MAPLE, soit en Macaulay2, soit en magma (ou en un tout autre langage), mais un autre point de vue est qu'il vaut mieux programmer une méthode dans un langage qui lui soit adapté : par exemple MAPLE ne convient absolument pas au calculs de bases de Gröbner, contrairement à Magma, qui explique le choix du langage pour la méthode de la section 6. D'un autre côté MAPLE est très efficace en ce qui concerne le factorisation de polynômes à plusieurs variables, et relativement performant en ce qui concerne l'algèbre linéaire.
L'idéal aurait été en fait de programmer toutes les méthodes en C ou en C++, mais cela aurait été une masse de travail trop importante pour un simple stage de 3 mois. Il faut donc relativiser les résultats numériques obtenus, d'autant plus que la durée d'exécution d'un algorithme sur un ordinateur peut varier en fonction de paramètres tels que par exemple la quantité de mémoire vive disponible au moment du calcul. Cependant les résultats obtenus permettent quand même de se faire une idée sur l'efficacité des méthodes testées.

Les temps de calculs sur chacun des exemples sont présentés dans un tableau.
• "Gröbner simple" désigne la méthode de la section 3.2.
• "Macaulay" désigne la méthode de la section 3.1 (exprimant l'équation implicite comme le quotient de deux déterminants D_n/D'_n).
• "Inversion" désigne la méthode permettant d'inverser une paramétrisation propre présentée à la section 4.1.
• "Algorithme Emiris-Sendra" désigne la méthode exposée à la section 4.2 et proposée par les deux chercheurs cités. Le temps du calcul de l'inverse N'EST PAS compté.
• "Algorithme simpliste" désigne le second algorithme proposé à la section 4.2. Là

aussi le temps du calcul de l'inverse N'EST PAS compté.
• "ASSIA" désigne la méthode de F. Aries et R. Senoussi présentée à la section 5. A priori on ne peut appliquer cette méthode qu'en l'absence de point base, mais on constate comme F. Aries et R. Senoussi qu'en présence de point base on obtient des multiples de l'équation implicite. Dans ces cas-là nous donnons deux temps : un principal qui correspond au temps de calcul d'un multiple de l'équation implicite ET de factorisation de celui-ci, et un deuxième entre parenthèses qui correspond au seul temps de la factorisation (si la factorisation n'est pas nécessaire le symbole "-" viendra remplacer le deuxième temps entre parenthèses).
• "Gröbner amélioré" désigne l'algorithme de O. Ruatta et P. Trebuchet expliqué à la section 6.
• "Surfaces mobiles" désigne selon le cas soit l'algorithme de la section 7.2, soit celui de la section 7.3.
• "Bezout" désigne la méthode présentée à la section 8 : le premier temps donné correspond au temps nécessaire pour trouver l'équation implicite exactement, ie le temps nécessaire pour calculer un mineur maximal du bezoutien ET factoriser celui-ci. Le temps entre parenthèses est le temps uniquement de la factorisation (si la factorisation n'est pas nécessaire,ie si le mineur calculé donne directement l'équation implicite, le symbole "-" viendra remplacer le temps entre parenthèses).
• "Résultant résiduel" désigne la méthode exposée à la fin de la section 9.2, et qui consiste à calculer un multiple de l'équation implicite et à le factoriser. Nous donnons encore une fois 2 temps : le premier correspond au temps total des opérations à effectuer pour trouver l'équation implicite (saturation+calcul d'un mineur maximal+factorisation); le deuxième, entre parenthèses, correspond au temps de la saturation.

Parfois certains calculs sont tellement longs que l'on est obligé de les interrompre : cela est aussi précisé dans les tableaux de résultats, avec le temps au bout duquel le calcul a été arrêté.
Les paramétrisations sont données sous la forme de 4 polynômes h_0,h_1,h_2,h_3 avec $x = \frac{h_1}{h_0}$,$y = \frac{h_2}{h_0}$,$z = \frac{h_3}{h_0}$.
La méthode basée sur le résultant résiduel tourne sous Macaulay2 : son code est disponible sur la page web de Laurent Buse. La méthode de Gröbner améliorée tourne sous Magma, et j'ai utilise le programme mis au point par O. Ruatta et P. Trebuchet. Les autres méthodes sont programmées en MAPLE, et les codes sont joint avec ce mémoire. Le bezoutien a été calculé à l'aide de la librairie "multires.mpl".

Exemple 1

$$\begin{cases} h_1(s,t) &= 3t + 3s^2t - t^3 \\ h_2(s,t) &= 3s + 3st^2 - s^3 \\ h_3(s,t) &= 3t^2 - 3s^2 \\ h_0(s,t) &= 1 \end{cases}$$

- **Degré de la paramétrisation=3.**
- **Degré de l'équation implicite=9.**
- **Sans point base.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium IV.**

Gröbner simple	1.7s
Macaulay	0.479s
Inversion	0.110s
Algorithme Emiris-Sendra	0.410s
Algorithme simpliste	0.640s
ASSIA	0.09s
Grobner amélioré	0.690
Surfaces mobiles	1.6s
Bezout	0,071
	(-)

Exemple 2

$$\begin{cases} h_1(s,t) &= 2s^3 + 13 + st^2 + 7ts^2 \\ h_2(s,t) &= 2t^3 + s^2 + 15 + 4s^2t + 6t + s^3 \\ h_3(s,t) &= 2t^2 + s + 17 + 9s^2t + 7t + s^2 \\ h_0(s,t) &= 2t^2 + s + 19 + 4s^2t + 7t + s^3 \end{cases}$$

- **Degré de la paramétrisation=3,**
- **Degré de l'équation implicite=9,**
- **Sans point base,**
- **Paramétrisation propre.**

– **Ordinateur utilisé : Pentium IV.**

Gröbner simple	arrêt à 3600s
Macaulay	forme indéterminée :0/0
Inversion	arrêt à 1500s
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	1.510s
Grobner amélioré	10.690s
Surfaces mobiles	5.120s
Bezout	7,771s
	(0.001s)

Commentaires :

Les deux déterminants D_n et D'_n sont nuls.

- L'"Algorithme Emeris-Sendra" et l'"Algorithme simpliste" n'ont pas pu être appliqué puisque l'inverse de la paramétrisation n'a pas pu être déterminé.

Exemple 3

$$\begin{cases} h_1(s,t) &= s^4 \\ h_2(s,t) &= t^4 \\ h_3(s,t) &= 2t^4 + 3s^2t^2 + 7t + 9s + 11 + 7st \\ h_0(s,t) &= 3s^4 + 4s^2t^2 + 5t + 7s + 11 + 9st + t^3 \end{cases}$$

– **Degré de la paramétrisation=4.**
– **Degré de l'équation implicite=16.**
– **Sans point base.**
– **Paramétrisation propre.**
– **Ordinateur utilisé : Pentium IV.**

Gröbner simple	arrêt à 3600s
Macaulay	forme indéterminée :0/0
Inversion	arrêt à 9 heures
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	105s
Grobner amélioré	1070s
Surfaces mobiles	2819s
Bezout	2908s
	(0.360s)

Commentaires :

identiques à ceux de l'exemple 2.

Exemple 4

$$\begin{cases} h_1(s,t) &= 32s^2t - 56st + 24t + 16s^3 - 120s^2 + 128s - 24 \\ h_2(s,t) &= 16t^3 - 16t^2 + 16st^2 + 48s^2t - 456st + 392t + 8s^2 + 384s - 392 \\ h_3(s,t) &= 64t^3 - 48t^2 + 48st^2 + 32s^2t - 1328st + 1232t + 16s^3 + 192s^2 + 1040s - 1248 \\ h_0(s,t) &= -6 + 4s - 6st + 2s^2 + 6t \end{cases}$$

- **Degré de la paramétrisation=3.**
- **Degré de l'équation implicite=4.**
- **Avec points bases.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium III.**

Gröbner simple	échec théorique
Macaulay	échec théorique
Inversion Algorithme Emiris-Sendra Algorithme simpliste	69s arrêt à 2200s 163s
ASSIA	0.250s (-)
Grobner amélioré	0.100s
Surfaces mobiles	échec théorique
Bezout	1.280s (-)
résultant résiduel	0.42s (0.069s)

Commentaires :

- La présence de points bases fait que certaines méthodes ne donneront jamais l'équation implicite (on a alors noté "échec théorique").

- Une fois l'inverse de la paramétrisation calculé (en 69s), sur les 163s nécessaires à l'algorithme simpliste pour trouver l'équation implicite seulement 22 seront consacrée à la factorisation de $num(Q_1 - x_1)$, contre 141 pour calculer la fraction rationnelle simplifiée Q_1.

- Cet exemple illustre bien la supériorité effective de l'algorithme dit "simpliste" sur l'algorithme de Emeris-Sendra.

Exemple 5

$$\begin{cases} h_1(s,t) &= 14004 - 7632t - 14004s + 7716st - 84s^2t^2 \\ h_2(s,t) &= 1692 - 972t - 1692s + 1056st - 84st^2 \\ h_3(s,t) &= 4284 - 3024t - 4284s + 3360st - 84st^2 - 252s^2t \\ h_0(s,t) &= 51 - 57s + 6s^2 + 6t \end{cases}$$

– **Paramétrisation de bidegré (2,2).**

- **Degré de l'équation implicite=5.**
- **Avec points bases.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium III.**

Gröbner simple	échec théorique
Macaulay	échec théorique
Inversion Algorithme Emiris-Sendra Algorithme simpliste	462s arrêt à 3600s 1752s
ASSIA	1.340s
Grobner amélioré	0.260s
Surfaces mobiles	échec théorique
Bezout	0.609s (-)
résultant résiduel	0.940s (0.050s)

Commentaires :

- La méthode de Macaulay échoue à cause des points bases. Même la méthode basée sur le résultant de Dixon ne donnerait pas l'équation implicite, car il y a ici d'autres points bases que les points bases canoniques en $(0:1:0)$ et en $(0:0:1)$.

- Une fois l'inverse de la paramétrisation calculé (en 462s), sur les 1752s nécessaires à l'algorithme simpliste pour trouver l'équation implicite seulement 471s seront consacrée à la factorisation de $num(Q_1 - x_1)$, contre 1283s pour calculer la fraction rationnelle simplifiée Q_1.

- C'est une nouvelle illustration de la supériorité effective de l'algorithme dit "simpliste" sur l'algorithme de Emiris-Sendra.

- On a aussi essayé de calculer l'équation implicite comme PGCD de tous les mineurs maximaux de la matrice M_ν (cf. 9.2) : une heure n'y aura pas suffit. C'est pourquoi nous avions expliqué à la fin de la section 9.2 qu'il valait nettement mieux calculer un seul de ces mineurs et le factoriser (ici cela prend 0.940s!!)

Exemple 6

$$\begin{cases} h_1(s,t) &= s^3+t^3+5st^2+2st-1 \\ h_2(s,t) &= 2s^2+2t^3+3st-2 \\ h_3(s,t) &= 5s^3+5t^2+3st^2+2s^2t+5st-5 \\ h_0(s,t) &= s^4+t^4-1 \end{cases}$$

- **Degré de la paramétrisation=4.**
- **Degré de l'équation implicite=10.**
- **Avec points bases.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium III.**

Gröbner simple	échec théorique
Macaulay	échec théorique
Inversion	arrêt au bout de 5000s
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	7.919s
	(-)
Grobner amélioré	38.250s
Surfaces mobiles	échec théorique
Bezout	113.640s
	(0.010s)
résultant résiduel	105.440s
	(0.189s)

Exemple 7

$$\begin{cases} h_1(s,t) &= 3t(t-1)^2+(s-1)^3+3s \\ h_2(s,t) &= 3s(s-1)^2+t^3+3t \\ h_3(s,t) &= -3s(s^2-5s+5)t^3-3(s^3+6s^2-9s+1)t^2+t(6s^3+9s^2-18s+3)-3s \\ h_0(s,t) &= 1 \end{cases}$$

- **Paramétrisation de bidegré (3,3), (c'est donc ce qu'on appelle une "bicubique")**

- **Degré de l'équation implicite=18.**
- **Sans point base.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium III.**

Gröbner simple	échec théorique
Macaulay	échec théorique
Inversion	arrêt au bout de 3600s
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	330s (0.5500s)
Grobner amélioré	399.55s
Surfaces mobiles	465s
Bezout	146s (-)
résultant résiduel	arrêt à 3 heures (0.445s)

Commentaires :

- On atteint là les limites de la méthode basée sur le résultant résiduel (la matrice obtenue est de taille 66×117).

Exemple 8

$$\begin{cases} h_1(s,t) &= s^3 + 2st^2 + 7ts + t^3 + 6t^2 \\ h_2(s,t) &= 3t^3 + 2s^2 + 5 + 7s^2 * t + 3t + s \\ h_3(s,t) &= t^2 + s + 5 + 2s^2t + 4t^2s \\ h_0(s,t) &= 2t^3 + s^2 + 9 + 4s^2t + 6t + s^3 \end{cases}$$

- **Degré de la paramétrisation=3.**
- **Degré de l'équation implicite=9.**
- **Sans point base.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium IV.**

Gröbner simple	arrêt à 1800s
Macaulay	au bout de 802s on obtient une forme indéterminée 0/0
Inversion	arrêt à 10 heures
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	1.420s
Grobner amélioré	8.120s
Surfaces mobiles	6.370s
Bezout	32,613s (0.171s)

Commentaires :

- Alors qu'ASSIA trouve l'équation implicite en 1,4s, plus de 10 heures ne suffiront pas à simplement calculer l'inverse de la paramétrisation, ce qui illustre bien un des points faibles de la méthode présenté au chapitre 4.

Exemple 9

$$\begin{cases} h_1(s,t) &= s^5 + t^2 - 3s + 2s^2t^2 - 2 - 4t - 2s^3 \\ h_2(s,t) &= 2t^2 + st^3 + 3s + 3t + 2 + s^3 \\ h_3(s,t) &= t^5 + 2s^2t^3 + 1 + 2s + 2t + s^3 \\ h_0(s,t) &= 1 + 2s + 2t + s^3 \end{cases}$$

- **Degré de la paramétrisation=5.**
- **Degré de l'équation implicite=25.**
- **Sans point base.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium IV.**

ASSIA	3267s
Surfaces mobiles	arrêt à 8 heures
Gröbner amélioré	arrêt à 6 heures

Commentaires :

- Seule la méthode ASSIA finit par aboutir à ce niveau de complexité des calculs (l'équation implicite est de degré 25!!)

Exemple 10

$$\begin{cases} h_1(s,t) &= 236567 * t1^2 + 476385 * t1 * t2 + 463578 * t2^2 + 208856 * t1 + 179962 * t2 + 123428 \\ h_2(s,t) &= 357568 * t1^2 + 104731 * t1 * t2 + 947734 * t2^2 + 986954 * t1 + 265889 * t2 + 983498 \\ h_3(s,t) &= 895567 * t1^2 + 38546 * t1 * t2 + 789556 * t2^2 + 126374 * t1 + 896578 * t2 + 478795 \\ h_0(s,t) &= 345190 * t1^2 + 248057 * t1 * t2 + 746956 * t2^2 + 982683 * t1 + 422317 * t2 + 593428 \end{cases}$$

- **Degré de la paramétrisation=2.**
- **Degré de l'équation implicite=4.**
- **Sans point base.**
- **Paramétrisation propre.**
- **Ordinateur utilisé : Pentium IV.**

Gröbner simple	arrêt à 1800s
Macaulay	44.15s
Inversion	arrêt à 1800s
Algorithme Emiris-Sendra	4684
Algorithme simpliste	4684
ASSIA	0.019s
Grobner amélioré	0.09
Surfaces mobiles	1.7s
Bezout	0,330s (0,080s)

10.2 Conclusion

Sur les exemples précédents il apparaît clairement que certaines méthodes d'implicitisation sont à éviter (à moins de tomber sur des cas vraiment simples) :

- La méthode appelée "Gröbner simple" ne trouve même pas en une demi-heure l'équation implicite de la paramétrisation de degré 2 de l'exemple 10 (certes celle-ci a de gros coefficients, mais ceci n'empêche d'autres méthodes d'aboutir très rapidement).

- La méthode "Macaulay", si elle est un peu plus performante (voir exemple 10), est toutefois elle-aussi très lente, et ne marche plus en présence de points bases. De plus, les exemples précédents ont souvent donné lieu à des formes indéterminées (cf. exemples 2,3,8).

- Pour ce qui est des méthodes basées sur la connaissance de l'inverse de la paramétrisation, leur premier gros problème est que l'inverse est rarement connu d'avance, et que calculer celui-ci par l'algorithme exposé à la section 4.1 est excessivement long. Cependant, même si on suppose l'inverse connu, les deux méthodes proposées n'en deviennent pas plus compétitives pour autant (voir les exemples 4 et 5). Trouver un algorithme d'inversion plus efficace ne suffirait donc pas à rendre ces méthodes intéressantes d'un point de vue numérique. L"'algorithme simpliste" apparaît toutefois bien meilleur que l"'algorithme Emiris-Sendra".

De toutes les méthodes testées, deux se distinguent particulièrement pour leur efficacité : "ASSIA" et "Gröbner amélioré". ASSIA est toutefois un peu plus adaptée aux paramétrisations sans point base (voir les exemples 2,8, et surtout 3 et 9) , tandis qu'au contraire "Gröbner amélioré" sera d'autant plus efficace qu'il y a de points bases (voir les exemples 4 et 5). Toutefois, dès que le degré de l'équation implicite dépasse 20, ces deux méthodes semblent atteindre leurs limites (voir exemple 9).
Les performances des méthodes basées sur les surfaces mobiles, les bezoutiens et les résultants résiduels semblent être, en général, légèrement en deçà des performances des deux méthodes précédentes (bien que sur certains exemples elles arrivent à rivaliser). Dans le cas de la méthodes des surfaces mobiles, il faut toutefois rappeler que l'on a traité que des cas sans point base; L. Busé, D. Cox et C. D'Andrea ont récemment travaillé sur une adaptation de la méthode en présence de points bases ([BCD]), et il serait intéressant de regarder ce que donne la méthode dans ce cas, car

comme nous l'avions signalé à la section 7.1 les points bases devraient augmenter la vitesse d'implicitisation.

11 Bibliographie

[AR]—F. Ariès et R. Senoussi, *An Implicitization Algorithm for Rational Surfaces with no Base Points*,J.Symbolic Computation (2001) 01, 1-9
[Baj]—C. Bajaj, T. Garrity and J. Warren, *On the applications of multiequational resultants*, Technical report CSD-TR-826, Department of Computer Science, Purdue University. nov. 1988
[BCD]—-L. Buse, D.Cox, C.D'Andrea, *Implicitization of surfaces in* $\mathbb{P}^3$ in the presence of base points, avec David Cox et Carlos D'Andréa, soumis, (Preprint).
[BEM]—L. Buse, M. Elkadi, B. Mourrain *Generalized Resultants over Unirationnal Algebraic Varieties*, J. Symbolic Computation (1999) 11,1-100. [Buse]—L. Buse. *Residual Resultant over the Projective Plane and the implicitisation Problem.*
[Castelnuovo]—G. Castelnuovo. *Sulla Razionalità Delle Involuzioni Piane.* Mathematishe Annalen, vol. 44, pp. 125-155.
[CGZ]—D.A.Cox, R.N.Goldman et M.Zhang, *On the validity of implicitization by moving quadrics for rationnal surfaces with no base points*, J.Symb.Comput.29 (2000), 419-440.
[Cox1]—D.Cox, J. Little and D. O'Shea. Ideals, *Varieties and Algorithms : An Introduction To Computational Algebraic Geometry And Commutative Algebra.* Undergraduate Texts in Mathematics. Springer Verlag, New York, 1992.
[D]—C.D'Andrea. *Resultants and moving surfaces.* J. Symbolic Computation (2001) 31, 585-602.
[Dix]—A.L.Dixon (1908) *The Eliminant of Three Quantics in Two Independant Variables.*
[H]—J. Harris (1992) *Algebraic geometry, a first course*, volume 133 of Graduate Texts in Math. Springer-Verlag.
[Hoff]—C. Hoffmann (1989) *Geometric and Solid Modeling : An Introduction*, Morgan Kaufmann Publishers Inc.
[Mac02]—F.S. Macaulay, *Some Formulae in Elimination*,Proc. London Math. Soc., Vol.35, 1902, pp.3-27.
[MayMey88]—E. Mayr, A. Meyer, *The complexity of the word problem for commutative semi-groups and polynomial ideals*, Adv. in Math. ,1998, vol. 127, p. 305-329.
[PDSS]—S.Pérez.Diaz, J. Schicho et J.R. Sendra, *properness and inversion of rationnal paramétrisations of surfaces.* Applicable Algébra in Engineering, Communication and Computing 13, pp. 29-51,2002.
[Sed90]—T.W. Sederberg, *Techniques for cubic algebraic surfaces*, IEEE CGA, ju juillet 1990, pp.14-25.

[shaf]—I.R. Shafarevitch, Basic Algebraic Geometry, Grundlehren 213, Springer-Verlag, 1984.

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399